I. OBJET ET DOMAINE D'APPLICATION

Le système d'information remplit des fonctions indispensables à la prise en charge des patients comme à la gestion quotidienne du CHU AMIENS PICARDIE et du GHT SLS. Sa disponibilité doit être assurée à tout moment et en toutes circonstances.

Certaines informations qu'il traite sont particulièrement sensibles, comme les données de santé des patients pris en charge et les données du personnel. Le système d'information doit garantir que ces informations restent authentiques et confidentielles. Son ouverture vers l'extérieur doit se faire dans un cadre sécurisé et maîtrisé.

Ces mêmes données sont exposées à des menaces et des risques réels, notamment de vol et de négligence, pouvant engager la responsabilité de tous.

En regard de ces risques, le CHU AMIENS PICARDIE et GHT SLS ont la responsabilité vis-à-vis des patients et vis-à-vis de l'État de garantir un niveau de sécurité suffisant pour protéger les données qui leurs sont confiées.

Pour relever ce défi, le CHU AMIENS PICARDIE a lancé une démarche en 2015 pour identifier les risques, élaborer et mettre en œuvre un plan d'action visant à permettre de maîtriser ces risques ; elle vise à renforcer les actions importantes déjà menées en protection du système d'information. Cette démarché est étendue au GHT SLS depuis sa mise en place.

La présente politique de sécurité des systèmes d'information constitue le cadre unique de référence du CHU AMIENS PICARDIE et GHT SLS pour toutes les questions de sécurité des systèmes d'information.

Chacun doit veiller personnellement à sa bonne mise en application, et faire preuve de vigilance dans son usage des moyens de traitement des informations. Chaque membre, chaque responsable de service doit communiquer cette politique et s'assurer que les exigences en matière de sécurité de l'information soient respectées au sein de son service et vis-à-vis de nos prestataires et sous-traitants.

A cette fin, je délègue au RSSI et RSMSI la responsabilité de mettre à jour les orientations de la politique de sécurité et je le désigne comme Responsable de la Sécurité des Systèmes d'Information et force de proposition des évolutions souhaitables de cette présente Politique de Sécurité des Systèmes d'Information au CHU AMIENS PICARDIE et sur le GHT SLS : Groupement Hospitalier de Territoire Somme Littoral Sud. Le RSSI doit promouvoir l'amélioration continue au sein du GHT SLS.

Amiens, le 31/01/2022
Madame la Directrice du CHU AMIENS PICARDIE

La Politique de Sécurité du Système d'Information (PSSI) du CHU AMIENS PICARDIE et du GHT SLS est un document de référence, validé par le RSSI et appuyé par la direction, qui doit être pris en compte par l'ensemble des acteurs et utilisateurs du système d'information.
Elle explicite les principaux enjeux de la sécurisation du système d'information pour le CHU AMIENS PICARDIE et le GHT SLS, elle fixe les exigences et les règles de sécurité qui permettent d'assurer cette sécurisation.
Les différentes mesures qu'elle prévoit permette de couvrir les risques identifiés lors des dernières analyses de risque.

Un plan d'action sécurité et un plan de traitement des risques sont suivis régulièrement afin de valider l'atteinte de la cible de sécurisation.

Cette présente PSSI s'applique à l'ensemble du périmètre d'information du CHU AMIENS PICARDIE et du GHT Somme Littoral Sud.

Tout le personnel est concerné : salarié, étudiant, stagiaire, intérimaire, prestataire, exerçant ses fonctions dans ou pour un établissement de santé du GHT SLS.

Tout le patrimoine informationnel est concerné par cette PSSI : ordinateur, serveur, équipement biomédical, applications métiers, papier, fax, copieur, téléphone, discussion, et les nouvelles technologies (objets connectés, ordiphones, tablettes, …).

Le document de la politique du SMSI complète et précise la PSSI sur le périmètre du SMSI.

II. DÉFINITIONS ET ABRÉVIATIONS

II.1 DEFINITIONS

Néant

II.2 ABREVIATIONS

ANAP : Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux

ANS (ex ASIP Santé) : Agence du Numérique en Santé (Systèmes d'Information Partagés de Santé)

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CNIL : Commission Nationale de l'Informatique et des Libertés

CPS : Carte de Professionnel de Santé

DGOS : Direction Générale de l'Offre de Soins

DMP : Dossier Médical Personnel

DNS : Domain Name System

DNSSEC : Domain Name System Security Extensions

GCS : Groupement de Coopération Sanitaire

GHT SLS : Groupement Hospitalier de Territoire Somme Littoral Sud

MAC : Media Access Control

MCO : Maintien en Conditions Opérationnelles

Plan d'action SSI : Plan d'Action Sécurité des Systèmes d'Information

PCA : Plan de Continuité d'Activité

PCI : Plan de Continuité Informatique

PDCA : Plan Do Check Act

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

PS : Professionnel de Santé

PSSI : Politique de Sécurité des Systèmes d'Information

RSSI ou RSMSI : Responsable de la Sécurité des Systèmes d'Information ou du Système de Management de la Sécurité de l'Information

SI ou DSN : Système d'information ou Direction des Services Numériques

SIS : Système d'Information de Santé

SMSI : Système de Management de la Sécurité de l'Information

SSID : Service Set Identifier

SSI : Sécurité des Systèmes d'Information

TCP/IP : Transmission Control Protocol / Internet Protocol

TLS : Transport Layer Security

WPA2 : Wifi Protected Access 2

III. DESCRIPTION

L'informatisation progressive du dossier patient, et potentiellement de tous les processus de production de soins (prescription, dispensation, administration), permet d'améliorer la sécurité et la qualité des soins dans le CHU AMIENS PICARDIE et le GHT SLS. Elle exige que le système d'information puisse fonctionner en continu (haute disponibilité : 24h/24 et 7j/7), conserver les données dans le temps tout en préservant leur intégrité, et garantir la confidentialité des informations médicales dans des environnements ouverts et partagés.

Dans le même temps, les systèmes d'informations du CHU AMIENS PICARDIE et du GHT SLS deviennent de plus en plus :

- Connectés : ils intègrent la gestion des équipements biomédicaux et l'exploitation des informations qu'ils produisent, les demandes d'accès au système d'information se diversifient avec l'usage de terminaux « mobiles » (smartphones, tablettes, ordinateurs portables) …
- Ouverts : pour favoriser la coordination des soins avec les autres acteurs de santé et permettre de mieux prendre en charge le patient tout au long de son parcours de soins : échange d'information médicale par messagerie sécurisée, partage de documents médicaux avec le DMP (Dossier Médical Personnel), Mon Espace Santé, coopération dans le cadre de réseaux de santé, développement de la télémédecine …
- Mutualisés dans le cadre de regroupements : GHT SLS, GCS, regroupement de cliniques liens avec ville hôpital, …

Le système d'information s'appuie sur un ensemble de plus en plus grand de dispositifs, interconnectés ou cohabitants, au service des professionnels de santé et pour le bénéfice d'une meilleure prise en charge du patient et d'amélioration du système de santé.

Levier d'amélioration de la qualité des soins et d'efficience, le SIH s'accompagne d'un accroissement significatif des vulnérabilités, des menaces et des risques d'atteinte aux informations conservées sous forme électronique et en conséquence aux processus de soins s'appuyant sur les systèmes d'information de santé. L'origine de ces menaces peut être intentionnelle (développement de la cybercriminalité, acte de malveillance d'un utilisateur du système d'information), ou involontaire (faille technique, manque de sensibilisation des utilisateurs…).

Dès lors, la sécurité de nos systèmes d'information est une condition indispensable pour garantir une bonne prise en charge des patients et une gestion intègre au CHU AMIENS PICARDIE et au GHT SLS.

La maîtrise de la sécurité des systèmes d'information doit être intégrée tout au long du cycle de vie de ces systèmes. Elle doit s'appliquer aux dispositifs et applications en place, et accompagner l'intégration des nouvelles applications ou de nouvelles procédures.
Elle doit prendre en compte l'évolution des facteurs, tant internes et qu'externes, qui sont susceptible de l'impacter : usage au quotidien des informations dématérialisées, stockage d'informations médicales à caractère personnel rendu facilement accessible, responsabilité de l'organisme quant au respect du décret confidentialité.

Elle doit en outre garantir la disponibilité des services du système d'information et offrir un socle de données fiables, intègres, et dont la confidentialité est protégée chaque fois que nécessaire.
La sécurité informatique doit s'inscrire dans une démarche « qualité » et de maîtrise global des risques, en recherchant l'adhésion des utilisateurs. Il est important de conserver à l'esprit que la capacité de protection et de réaction repose bien souvent in fine sur l'utilisateur.

Cadre législatif et règlementaire

La plupart des textes qui s'appliquent au SIH de l'établissement sont codifiés dans les codes suivants :

- code de la santé publique ;
- code de l'action sociale et des familles ;
- code des postes et télécommunication ;
- code du patrimoine ;
- code civil ;
- code pénal.

Il convient de ne pas omettre le respect de règles de la Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Normes et documents de référence

Les textes mentionnés ci-après s'imposent aux structures qui relèvent du secteur public et doivent être pris en compte pour l'élaboration et la mise en œuvre de la PSSI :

- Référentiel Général de Sécurité (RGS) [Réf. n°9] ;
- Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) [Réf. n°10].

Les textes mentionnés ci-après ne sont pas de nature impérative, mais sont utiles comme références pour l'élaboration ou la mise en œuvre de la PSSI :

- Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) – Principes fondateurs (ANS, ex ASIP Santé) et corpus documentaire associé [Réf. n°6] ;
- ISO 27002 [Réf. N°11].

L'annexe 6 présente la correspondance entre les thématiques d'exigences et de règles utilisées par ce guide et :

- les actions pour atteindre les prérequis du programme Hôpital Numérique [Réf. n°3bis] ;
- les objectifs de sécurité fixés par la PSSIE [Réf. n°10] ;
- *les articles de la norme ISO 27002 [Réf. N°11].*

Table des matières

Gestion des risques du SI

Pour créer une politique efficace en matière de sécurité de l'information, une approche systématique de la gestion des risques de la sécurité des systèmes d'information a été définie afin d'identifier les besoins des membres du GHT SLS en matière de sécurité de l'information.

Une approche spécifique de la gestion des risques de la sécurité des SI a été définie pour le Système de Mangement de la Sécurité du Système d'Information du GHT SLS.

La méthode d'évaluation des risques doit fournir une approche périodique, cohérente et systématique pour estimer le niveau des risques et les comparer aux critères d'acceptation, ceci afin d'évaluer leur importance et évolution dans le temps. La gestion des risques liée à la sécurité de l'information est un processus continu. Le processus devrait établir le contexte externe et interne, évaluer les vulnérabilités, les menaces et traiter les risques en utilisant un plan de traitement des risques.

Objectifs de sécurité

Selon les analyses de risques effectuées sur les différents périmètres et sa stratégie de GHT, des objectifs de sécurité ont été définis afin de contribuer aux objectifs stratégiques de sécurité du GHT SLS.

Ces objectifs se traduisent par les points suivants :

- Garantir une disponibilité des applications conformément au besoin du métier
- Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information du GHT SLS.
- Se protéger de la perte de données
- Empêcher toute exploitation des vulnérabilités techniques.
- Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.
- Engager les utilisateurs à utiliser de manière sécurisé les moyens de traitement de l'information
- Empêcher les accès externes non autorisés aux systèmes et aux applications.
- S'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information.
- Effectuer régulièrement une gestion des risques en relation avec le service qualité
- S'assurer du traitement des non-conformité et des actions correctives
- Assurer un niveau adéquat de protection des données à caractère personnelle et protéger les informations personnelles qui sont collectées, traitées et gérées conformément à l'activité qui consiste à fournir des services d'infogérance et d'hébergement aux membres du GHT SLS.

La cohérence et l'avancement dans l'atteinte de ces objectifs sont suivis lors des groupes thématiques système d'information avec la qualité.

Exigences de sécurité et règles applicables

Format de présentation des exigences

Organisation des exigences par thématique

Les exigences sont structurées selon 7 thématiques :

- Thématique 1 : Répondre aux obligations légales
- Thématique 2 : Promouvoir et organiser la sécurité
- Thématique 3 : Assurer la sécurité physique des équipements informatiques du SI
- Thématique 4 : Protéger les infrastructures informatiques
- Thématique 5 : Maîtriser les accès aux informations
- Thématique 6 : Acquérir des équipements, logiciels et services
- Thématique 7 : Limiter la survenue et les conséquences d'incidents de sécurité

Pour chaque thématique, une ou plusieurs sous-thématiques sont définies. Chacune d'elle énonce un ensemble d'exigences.

Pour chaque exigence, une formulation détaillée de l'exigence est posée, éventuellement précédée d'un paragraphe à but didactique. Les règles applicables associées sont ensuite formulées.

Les exigences présentent la cible de sécurité à atteindre. A chaque exigence, une ou plusieurs règles est associé.

A chaque règle est associée une référence qui l'identifie (voir chapitre 5.1.3 plus bas) et une indication des catégories de moyens du SI auxquelles la règle doit être appliquée.

Pour chaque règle, le terme « devoir » ou « obligation » défini une règle qui doit être appliquée obligatoirement dans le cadre défini. Toute dérogation à ce principe doit être validée, délimitée dans le temps et tracée (dans un référentiel unique) par la commission habilitation et sécurité. Une revue annuelle doit être faite par la commission habilitation et sécurité afin de renouveler chaque dérogation. La revue des dérogations périmées ou sur le point de l'être doit être faite en commission habilitation et sécurité.
Le terme « devrait » fait référence à une préconisation.
Dans un esprit d'amélioration continue, une action sécurité peut être associé à chaque règle, le tout, regroupé dans un plan d'action sécurité, la réalisation de l'action permet de passer la règle d'une préconisation à une obligation lors de la mise à jour de la PSSI.

Thématique 1 : Répondre aux obligations légales

La dématérialisation des données de santé et la mise en œuvre d'un SI au sein d'une structure du secteur sanitaire ou médico-social doit s'effectuer dans le respect de la réglementation applicable.
En particulier, l'obligation de secret professionnel doit être respectée quel que soit le support de l'information de santé, papier ou informatique. Dans ce sens, chaque structure doit au moins assurer aux informations de santé dématérialisées le même niveau de protection et de confidentialité que celui qu'elle donne aux informations conservées sous forme papier.

T1-1 Respecter les principes de la protection des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définit les principes à respecter lors de la collecte, du traitement et de la conservation des données à caractère personnel.

Ces principes sont au nombre de cinq :

⇒ **la finalité du traitement**

Les données à caractère personnel ne peuvent être collectées et traitées que pour une finalité validée, déterminée, explicite et légitime. Elles ne peuvent être utilisées de manière incompatible avec cette finalité. Le détournement de finalité peut être sanctionné pénalement.

⇒ **la pertinence et la proportionnalité des données**

Les données collectées et traitées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

Certaines catégories de données font l'objet d'une protection légale particulière, notamment les données identifiées comme « sensibles[1] » dont font partie les données de santé à caractère personnel (art. 8).

⇒ **la conservation limitée des données**

Les données ne peuvent être conservées dans les fichiers au-delà de la durée nécessaire à la réalisation de la finalité poursuivie.

⇒ **la sécurité et la confidentialité des données**

Le responsable du traitement doit veiller à ce que les données ne soient pas déformées, endommagées et que des tiers non autorisés ne puissent y avoir accès.

Les mesures de sécurité physique et logique doivent être adaptées à la nature des données et aux risques présentés par le traitement.

⇒ **le respect des droits des personnes**

- le droit à l'information,
- le droit d'opposition et liée au profilage,
- le droit d'accès,
- le droit d'effacement,
- le droit de rectification,
- le droit de portabilité,

[1] Les « données sensibles » sont, par exemple, les données de santé à caractère personnel, les autres données à caractère personnel, ou toutes autres données jugées sensibles dans le cadre d'une analyse de risque.

- la demande de limitation,
- la notification de la personne concernée,
- les procédures de gestion de ces demandes et droits.

L'exercice de ces droits est soumis à certaines conditions fixées par la loi informatique et libertés et son décret d'application (Décret n°2005-1309 du 20 octobre 2005).

En outre, tout responsable de traitement ne peut mettre en œuvre un traitement automatisé contenant des données à caractère personnel qu'après s'être assuré du respect des formalités préalables applicables, le cas échéant, à la mise en œuvre du traitement.

A cet effet, un Délégué à la Protection des Données (DPO) a été nommé en mai 2018 au sein du CHU AMIENS PICARDIE et GHT SLS ainsi qu'une équipe conformité RGPD et sécurité numérique avec le RSSI et les RIL.

T1-1.1 Respecter les procédures préalables au sein de la structure ou devant la CNIL (déclaration ou autorisation des traitements de données à caractère personnel)

Exigences :

⇒ Tout traitement de données à caractère personnel doit être mis au registre du GHT, et au besoin déclaré à la CNIL pour être autorisé par celle-ci, selon la nature des données concernées et l'analyse d'impact sur la vie privée.

Déclinaison en règles :

Règles sur les demandes d'autorisations préalables ou déclarations de la conformité auprès de la CNIL :

Réf.	Règles	Catégories de moyens du SI concernées
1.1.1.1	La mise en œuvre de toute nouvelle fonctionnalité (i.e. nouvelle application, nouvelle fonctionnalité d'une application existante…) doit être analysée pour déterminer si elle nécessite une modification de la déclaration ou de la demande d'autorisation[2] de la structure. Le cas échéant, la déclaration ou la demande d'autorisation de la structure doit être mise à jour[3] pour intégrer cette évolution des traitements de données à caractère personnel mise en œuvre par la structure.	*Logiciels*
1.1.1.2	La déclaration ou la demande d'autorisation de la structure doit être régulièrement[4] revue pour vérifier qu'elle décrit correctement les traitements de données à caractère personnel mis en œuvre au sein de la structure.	*Logiciels*

[2] http://www.cnil.fr/vos-obligations/vos-obligations/

[3] http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/mode-demploi/comment-declarer/la-demande-dautorisation/

http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/

[4] La fréquence de révision est à déterminer en fonction du rythme des évolutions du système d'information. Une revue annuelle ou bisannuelle est conseillée.

	Le cas échéant, la déclaration ou la demande d'autorisation doit être mise à jour pour refléter l'ensemble des traitements de données à caractère personnel.	

T1-1.2 Sensibiliser le personnel aux enjeux concernant les données à caractère personnel

Exigences :

⇒ Toute personne amenée à participer à un traitement de données à caractère personnel doit être sensibilisée aux principes de protection de ce type de données.

Déclinaison en règles :

Règles sur la sensibilisation :

Réf.	Règles	Catégories de moyens du SI concernées
1.1.2.1	Toute personne amenée à avoir accès à des données à caractère personnel doit être sensibilisée à la protection de ces données et en particulier à leur confidentialité. Cette sensibilisation intervient dans les 6 mois de la prise de fonction de la personne et fait l'objet d'une mise à jour régulière par des sessions « piqures de rappel ». Cette sensibilisation prend également la forme de diffusion de mail de communication en cas d'alerte de sécurité, de sessions par le RSSI et le DPO pour des demandes ciblées, ou lors des formations aux outils du système d'information.	*Services (ex. Service des urgences), Catégorie de personnel (ex. Professionnel de santé)*
1.1.2.2	L'ensemble du personnel du GHT SLS et de ses membres est informé de la collecte de traces, par les SI, de tout accès à des données à caractère personnel et de la possible mise en œuvre de contrôles *à posteriori* sur les accès tracés et sur leur bien fondé.	*Services, Catégorie de personnel*
1.1.2.3	Toute personne en charge de l'achat des applications, de la définition du paramétrage des applications et/ou de la définition des spécifications fonctionnelles des applications doit être sensibilisée aux notions de pertinence et de proportionnalité des données pour qu'elle pense à limiter les données collectées aux données strictement nécessaires aux traitements mis en œuvre. Cette sensibilisation doit intervient dans les 6 mois de la prise de fonction de la personne et fait l'objet d'une mise à jour régulière par des « piqûres de rappel » par le DPO.	*Services, Catégorie de personnel*

T1-1.3 Respecter les droits des personnes

Exigences :

⇒ Toute personne dont des données à caractère personnel sont traitées par la structure doit pouvoir exercer les droits qui y sont associés (droit à l'information, droit d'opposition, droit d'accès et droit de rectification).

Déclinaison en règles :

Règles sur le respect des droits des personnes :

Réf.	Règles	Catégories de moyens du SI concernées
1.1.3.1	Des procédures doivent être mises en œuvre pour permettre, pour les données à caractère personnel traitées pour chaque structure : • l'opposition d'une personne à la collecte de données à caractère personnel la concernant ; • l'accès d'une personne aux données à caractère personnel la concernant ; • la rectification par une personne des données à caractère personnel la concernant.	*Services (ex. Service d'accueil), logiciels*
1.1.3.2	Tout personnel amené à être en contact avec des personnes dont des données à caractère personnel sont traitées par les structures doit être informé des procédures mentionnées dans la règle 1.1.3.1.	*Catégorie de personnel (ex. Professionnels de santé)*
1.1.3.3	Des éléments d'information à destination des personnes concernées sur leurs droits d'opposition, d'accès et de rectification et la manière d'exercer ces droits doivent être rédigés et maintenus à jour.	*Catégorie de personnel*
1.1.3.4	Les procédures internes, impliquant la collecte et le traitement de données à caractère personnel, doivent prévoir une étape d'information des personnes concernées basée sur les éléments d'information mentionnés dans la règle 1.1.3.3. Les informations sont réalisées oralement, ou par la diffusion d'une documentation dans laquelle le sujet est abordé (ex. livret d'accueil) et par des affiches aux guichets d'accueil ainsi que le site Internet de chaque structure.	*Services*

T1-2 Respecter les règles d'échange et de partage de données de santé à caractère personnel

L'article L 1110-4 du code de la santé publique ainsi que le décret n° 2007-960 du 15 mai 2007 codifié au code de la santé publique posent les grands principes d'échange et de partage des données de santé à caractère personnel et les modalités de mise en œuvre de la sécurité des SI associés.

L'échange ou le partage d'informations concernant un usager est autorisé entre les professionnels le prenant en charge, dans l'intérêt même de l'usager. L'usager doit cependant en être informé et son consentement recueilli.

En substance, toute prise en charge d'un usager doit débuter par une information de l'usager sur la possibilité d'échange et de partage des données de santé à caractère personnel le concernant et, sauf exception prévue par la loi (ex. recherche clinique acceptée par le usager), l'accès à toute donnée de santé à caractère personnel doit être limitée aux personnes participant à la prise en charge de l'usager correspondant (soin, continuité des soins, détermination de la meilleure prise en charge sanitaire possible…).

T1-2.1 Informer l'usager et recueillir son consentement

Exigences :

⇒ Tout usager pris en charge doit être informé des possibilités, dans le cadre de sa prise en charge, d'échange et de partage de données de santé à caractère personnel le concernant.

Déclinaison en règles :

Règles sur l'information de l'usager :

Réf.	Règles	Catégories de moyens du SI concernées
1.2.1.1	Des éléments d'information à destination des usagers sur les conditions de partage et d'échange de leurs données de santé à caractère personnel dans le cadre de leur prise en charge doivent être rédigés et maintenus à jour.	*Catégorie de personnel*
1.2.1.2	La procédure de prise en charge des usagers doit être formalisée et documentée et intégrer une étape d'information de l'usager fondée sur les éléments d'information des règles 1.2.1.1 et 1.1.3.3 ainsi qu'une étape de recueil du consentement de l'usager quel qu'en soit le moyen (écrit ou dématérialisé). L'information est réalisée oralement et par la diffusion d'une documentation dans laquelle le sujet est abordé. Elle est complétée par des affiches d'information dans les locaux[5]. En particulier, pour les établissements de santé, ces éléments doivent figurer dans le livret d'accueil tel que décrit dans l'article R1112-9 du code de la santé publique.	*Catégorie de personnel (ex : Personnel d'accueil, Professionnels de santé)*

T1-2.2 Limiter l'accès aux données de santé à caractère personnel aux personnes participant à la prise en charge

Exigences :

⇒ En fonctionnement nominal, seules les personnes participant à la prise en charge sanitaire d'un usager peuvent avoir accès aux données de santé à caractère personnel le concernant.

Déclinaison en règles :

Règles sur la limitation des accès aux données de santé à caractère personnel :

[5] La CNIL propose des modèles d'affiches de ce type. Certains services nationaux peuvent également mettre à disposition des modèles d'affiche pour les structures qui les utilisent (ex. affiche de sensibilisation au DMP mise à disposition par l'ANS, ex ASIP Santé).

Réf.	Règles	Catégories de moyens du SI concernées
1.2.2.1	Les personnels participant à la prise en charge sanitaire des usagers devraient être formés aux conditions de partage et d'échange des données de santé à caractère personnel en particulier avec l'extérieur.	*Catégorie de personnel*
1.2.2.2	Une liste de professionnels de santé dûment habilités à intervenir de façon exceptionnelle sur des données de santé à caractère personnel en dehors de la prise en charge sanitaire de l'usager (par exemple dans le cadre de la résolution d'incident) doit être élaborée et maintenue à jour.	*DIM de territoire*

T1-3 Répondre aux obligations de conservation et de restitution des données

T1-3.1 Fixer une durée de conservation des données à caractère personnel

Exigences :

⇒ Toute donnée à caractère personnel ne doit être conservée que pendant une durée cohérente avec la finalité du traitement pour lequel elle a été collectée.

⇒ La conservation de données de santé à caractère personnel doit par ailleurs respecter les durées indiquées par la loi lorsque celles-ci sont spécifiées.

Déclinaison en règles :

Règles sur la durée de conservation des données à caractère personnel :

Réf.	Règles	Catégories de moyens du SI concernées
1.3.1.1	Pour chaque type de donnée à caractère personnel traitée, une durée de conservation doit être clairement établie, documentée dans une annexe de la PSSI (cf. modèle en annexe 2) et indiquée dans les déclarations CNIL correspondantes (cf. exigence T1-1.1).	*Organisation (ex. Direction de l'Information Médicale)*
1.3.1.2	Les règles et procédures de gestion et d'archivage des données devraient tenir compte de la durée de conservation des données à caractère personnel.	*Organisation*

T1-3.2 Respecter les règles relatives à l'hébergement de données de santé à caractère personnel

Exigence :

⇒ Des données de santé à caractère personnel ne peuvent être confiées qu'à un organisme tiers[6] disposant d'un agrément ou certification en tant qu'hébergeur de données de santé à caractère personnel.

Déclinaison en règles :

Règles sur le recours à un tiers pour l'hébergement de données de santé à caractère personnel :

[6] Par exemple dans le cadre d'une prestation de fourniture d'un outil en ligne de gestion des patients

Réf.	Règles	Catégories de moyens du SI concernées
1.3.2.1	Tout transfert de données de santé à caractère personnel à un organisme tiers est soumis à une contractualisation préalable avec ce tiers pour l'hébergement de ces données.	*Organisation (ex. Direction de l'Information Médicale, Responsable de la SSI)*
1.3.2.2	Toute contractualisation avec un tiers pour l'hébergement de données de santé à caractère personnel requiert que ce tiers détienne un agrément ou une certification reconnu par l'Etat Français en tant qu'hébergeur de données de santé à caractère personnel, valide à la date de signature du contrat. Le tiers doit transmettre toute référence utile permettant la vérification de la validité et de la date d'expiration de cet agrément ou certification. Le contrat doit intégrer des dispositions à activer en cas de non renouvellement de l'agrément pendant la durée du contrat	*Organisation*

T1-4 Veille réglementaire

T1-4.1 Assurer une veille réglementaire des dispositions applicables à la structure en matière de SSI

Exigence :

⇒ Les évolutions légales et règlementaires en matière de sécurité des systèmes d'informations ainsi que les jurisprudences dans le domaine doivent être traduites dans la PSSI si elles s'appliquent à la structure.

Déclinaison en règles :

Règles sur la veille règlementaire :

Réf.	Règles	Catégories de moyens du SI concernées
1.4.1.1	Une veille règlementaire doit être réalisée avec une fréquence mensuelle au minimum. Elle concerne les thématiques relatives à la sécurité des systèmes d'information de santé, qui couvre au moins : ○ La sécurité des systèmes d'information ; ○ Le traitement des données à caractère personnel ; ○ Les conditions d'échanges et de partage de données de santé à caractère personnel ; ○ Les conditions de conservation des données de santé à caractère personnel ; Les référentiels de sécurité des SI applicables aux secteurs sanitaire et médico-social en particulier ceux visés par l'article L. 1110-4-1. Cette veille est réalisée en interne par les services impactés et concernés.	*Service (ex. Direction juridique), Catégorie de personne (ex. Responsable de la SSI)*

Thématique 2 : Promouvoir et organiser la sécurité

T2-1 Définir une organisation pour la mise en œuvre de la SSI au sein de la structure

T2-1.1 Identifier les acteurs de la politique de sécurité de la structure et leurs activités

Exigence :

⇒ Chacune des fonctions de sécurité suivantes doit être attribuée à une personne identifiée :

- Elaboration et maintenance de la PSSI ;
- Pilotage de la mise en œuvre de la PSSI et contrôle de son application effective ;
- Gestion des incidents SSI.

Déclinaison en règles :

Règles sur l'identification des acteurs :

Réf.	Règles	Catégories de moyens du SI concernées
2.1.1.1	Un Responsable de la SSI est désigné depuis 2004 au sein du CHU AMIENS PICARDIE. Le Responsable de la SSI est responsable de l'élaboration de la PSSI, de l'organisation de sa mise en œuvre via le *Plan d'action SSI* et du suivi de son application.	*Catégorie de personnel (ex. Direction de la structure)*
2.1.1.2	Le Responsable de la SSI doit piloter la rédaction de la PSSI de la structure et la maintenir à jour. En particulier, il doit intégrer les nouvelles mesures de sécurité éventuelles validées dans le cadre de la règle 2.1.2.2	*Catégorie de personne (ex. Responsable SSI)*
2.1.1.3	Le Responsable de la SSI doit coordonner l'élaboration des *Plans d'action SSI* successifs de la structure selon les principes décrits dans le guide d'élaboration et de mise en œuvre d'une PSSI [Réf. n°6.1]. En particulier, il doit intégrer les éventuelles nouvelles mesures de sécurité validées dans le cadre de la règle 2.1.2.2 et identifiées comme devant être mises en œuvre dans le *Plan d'action SSI* courant.	*Catégorie de personne*
2.1.1.4	Le Responsable de la SSI doit suivre la mise en œuvre des *Plans d'action SSI* successifs et en présenter l'avancement lors des réunions identifiées dans le thème T2-1.2.	*Catégorie de personne*
2.1.1.5	Le Responsable de la SSI devrait régulièrement contrôler que les règles mises en œuvre dans le cadre des *Plans d'action SSI* successifs sont toujours respectées.	*Catégorie de personne*
2.1.1.6	Le Responsable de la SSI doit piloter les actions de sensibilisation et de formation à la sécurité décrites dans le thème T2-2	*Catégorie de personne*
2.1.1.7	Le Responsable de la SSI devrait coordonner et vérifier l'intégration et le respect des clauses liées à la SSI lors de contractualisation, mise en place de conventions ou	*Catégorie de personne*

	acquisition d'équipements, logiciels et services, selon les règles énoncées dans le thème T6. Il devrait également veiller à l'actualisation de ces mêmes types de contrats et conventions existants afin qu'y soient intégrés les règles du thème T6.	
2.1.1.8	Un Référent Incident SSI doit être désigné. Le Référent Incident SSI est responsable de la gestion des incidents qui mettent à mal la sécurité du SI ou qui révèlent une défaillance des mesures SSI, de leur résolution ainsi que des retours d'expérience qui peuvent en être déduits. Les tâches du Référent Incident SSI sont spécifiées par les règles du thème 7-3.	*Catégorie de personne*
2.1.1.9	A chaque réunion identifiée dans le thème T2-1.2, le Référent Incident SSI doit présenter une synthèse des éventuels incidents qui ont eu lieu depuis la réunion précédente ainsi que les propositions de mesures élaborées dans le cadre de la règle 7.3.3.2.	*Catégorie de personnel*
2.1.1.10	Un Référent Plan de Continuité Informatique (Référent PCI) doit être désigné. Les tâches du Référent PCI sont spécifiées par les règles du thème 7-5.	*Catégorie de personnel (ex. Direction de la structure)*
2.1.1.11	Une autorité d'homologation SSI devrait être constituée, L'homologation est l'acte selon lequel le responsable du SI atteste formellement que le système d'information est protégé conformément aux objectifs de sécurité fixés. L'autorité d'homologation doit rassembler les différents responsables métiers de SI de la structure, le responsable informatique au titre des composants d'infrastructure partagés et le Responsable de la SSI qui veille à la cohérence de la sécurité du SI global. Le Référent PCI et le Référent Incident SSI peuvent être associés à titre consultatif à l'autorité d'homologation.	*Catégorie de personnel (ex. Direction de la structure)*

T2-1.2 Formaliser les remontées d'informations sur la sécurité à la direction

Exigence :

⇒ La direction doit être informée des incidents touchant le système d'information et des mesures mises en œuvre pour sécuriser celui-ci.

Déclinaison en règles :

Règles sur l'information de la direction :

Réf.	Règles	Catégories de moyens du SI concernées
2.1.2.1	La sécurité doit être inscrite à l'ordre du jour d'une réunion de pilotage récurrente à laquelle participe la direction de la structure. La réunion se tient avec une fréquence semestrielle au minimum.	*Catégorie de personne (ex. Responsable de la SSI)*
2.1.2.2	Lors des réunions identifiées dans la règle 2.1.2.1, les éléments suivants (au minimum) devraient être présentés :	*Catégorie de personne*

	• au lancement de chaque itération du *Plan d'action SSI* : le périmètre du projet ; • suivi de la mise en œuvre du *Plan d'action SSI* ; • synthèse des incidents sur la période ; • éventuellement, recommandations de nouvelles mesures de sécurité, suite au retour d'expériences sur les incidents. Le cas échéant, les décisions suivantes sont prises : • validation du périmètre du *Plan d'action SSI* lors de son lancement ; • décision de mise en œuvre ou non des recommandations de nouvelles mesures de sécurité et d'intégration dans le *Plan d'action SSI* courant ou de planification de mise en œuvre dans un *Plan d'action SSI* ultérieur. Les informations de suivi de la sécurité du SI qui sont présentées au cours de cette réunion peuvent l'être sous forme de tableau de bord, présentation synthétique des informations principales, avec le cas échéant leur évolution dans le temps. Le guide [Réf. n°8] propose une méthode d'élaboration de tableau de bord de sécurité du SI.	

T2-2 Faire connaître les principes essentiels de sécurité informatique

T2-2.1 Sensibiliser, former et responsabiliser le personnel

Exigence :

⇒ Le personnel de la structure doit être sensibilisé aux enjeux sécurité et devrait être formés aux bonnes pratiques de sécurité à mettre en œuvre.

Déclinaison en règles :

Règles sur la sensibilisation du personnel :

Réf.	Règles	Catégories de moyens du SI concernées
2.2.1.1	Une charte d'utilisation des ressources informatiques doit être élaborée et devrait être diffusée à tout utilisateur du système d'information, qu'il s'agisse de personnel interne ou de tiers amenées à utiliser le SI ou à intervenir sur le SI. Il est recommandé que cette charte soit rendue opposable à tout utilisateur du SI, par exemple par une acceptation individuelle explicite (notamment pour les utilisateurs ne faisant pas partie du personnel permanent) ou par une intégration de la charte au règlement intérieur de la structure. Les procédures préalables de validation de la charte par les instances de décision et de consultation des instances représentatives du personnel éventuellement prévues par la règlementation ou les conventions applicables à la	*Catégorie de personnel (ex. Responsable de la SSI, Direction de la structure)*

	structure doivent bien évidemment être respectées dans le cadre cette action.	
2.2.1.2	Les éléments sécurité présentés dans la charte d'utilisation devraient faire l'objet de très courts rappels des règles et bonnes pratiques abordant au minimum : • les principes de sécurisation des mots de passe (voir T4-5.1) ; • les principes de protection de l'accès aux postes de travail (voir T4-5.2) ; • la liste des catégories de données considérées comme sensibles ou leurs critères de catégorisation (par exemple : les données de santé à caractère personnel, les autres données à caractère personnel, les données participant à la sécurité du SI, ou toutes autres données jugées sensibles dans le cadre d'une analyse de risque) ; • les règles d'accès aux données sensibles (voir T5-1.1) et en particulier les règles d'accès aux données de santé à caractère personnel ; • les règles relatives à l'usage d'Internet au sein de la structure (voir T4-3.2) ; • les types de situations vis-à-vis desquelles les utilisateurs doivent être vigilants du point de vue SSI et les principes d'alerte du Référent en cas d'incident (voir T7-3.2).	*Catégorie de personnel*
2.2.1.3	Les personnels en charge de l'administration et de l'exploitation des infrastructures et des applications du SI doivent être formés à la réalisation des tâches qui leur incombent, pour chacun des composants dont ils ont la charge, et notamment : • installation et réinstallation ; • exploitation régulière ; • sauvegarde et restauration des configurations et des données ; • détection des anomalies d'exploitation et de sécurité ; • traitement des incidents d'exploitation et de sécurité ; • procédures de continuité de fonctionnement.	*Equipe DSN*
2.2.1.4	Les utilisateurs du SI doivent être formés à l'utilisation des équipements et applications du SI qui leur sont destinés. Outre les aspects fonctionnels métiers de ces composants, ils doivent être formés : • aux procédures d'authentification et de gestion de leurs moyens d'authentification ; • à la vigilance vis-à-vis d'anomalies qui pourraient révéler un problème de sécurité du SI ; • aux modalités d'accès et de protection des données sensibles, • à la procédure d'alerte en cas de perte, vol ou disparition de tout composant du SI, et en particulier d'un support contenant des données sensibles ;	*Catégorie de personne (ex : tout utilisateur du SI)*

	• aux éventuelles procédures de fonctionnement dégradé en cas d'activation du PCA.	
2.2.1.5	Les opérations de formation doivent être réalisées sur un environnement de formation dédié (au moins temporairement) à cet usage (i.e. elles ne doivent pas être effectuées sur les postes de travail et équipements utilisés pour la production).	*Catégorie de personne (ex : Chargé de formation)*

T2-2.2 Décliner les règles de la PSSI dans les procédures opérationnelles

Exigence :

⇒ Les procédures opérationnelles de la structure devraient intégrer explicitement les aspects sécurité du SI.

Déclinaison en règles :

Règles sur la déclinaison des règles de sécurité :

Réf.	Règles	Catégories de moyens du SI concernées
2.2.2.1	Les aspects sécurité du SI devraient être intégrés aux procédures de la structure en tant qu'étape fonctionnelle au même titre que les aspects métiers. Une revue initiale des procédures existantes, puis de toute nouvelle procédure, devrait être menée dans ce sens afin de vérifier que les règles fixées par la PSSI sont toutes prises en compte et déclinées au niveau opérationnel. Si nécessaire, les procédures doivent être amendées, et de nouvelles procédures doivent être crées le cas échéant.	*Catégorie de personnel (ex. responsables du service informatique)*
2.2.2.2	La procédure d'embauche ou d'arrivée de personnel temporaire ou de prestataire devrait intégrer les étapes sécurité suivantes : • remise de la charte d'utilisation des ressources informatiques ; • le cas échéant, remise de matériel informatique et signature du registre de prise en charge de matériel ; • le cas échéant, remise de moyen(s) d'authentification lié à la/aux fonction(s) (ex. CDE) et des consignes d'utilisation. (ex. notice explicative relative aux conditions générales d'utilisation des cartes de la famille CPx, accessible sur le site esante.gouv.fr) ; • le cas échéant, remise de moyen(s) d'accès aux locaux (clés, cartes, …) requis ; • sensibilisation aux problématiques et enjeux de la SSI ; • formation aux règles de gestion des mots de passe et de la sécurité des postes de travail telles que présentées dans les thèmes 4-5.1 et 4-5.2 et	*Catégorie de personnel (ex. Direction du personnel, Responsable de la SSI)*

	coordonnées des personnes à contacter en cas d'oubli du mot de passe ; • présentation des règles d'alerte en cas d'incident telles que présentées dans le thème 7-3.2 et des coordonnées des personnes à contacter en cas d'incident ; • détermination du/des profil(s) utilisateur(s) du/de la nouvel(le) embauché(e) correspondant à sa/ses fonction(s) tel que présenté dans le thème 5-1.1 ; • création du/des compte(s) nominatif(s)[7] du/de la nouvel(le) embauché(e) dans le système d'information et attribution des droits d'accès correspondant à son/ses profil(s) utilisateur(s) ; • sensibilisation aux aspects sécurité telle que présentée à la règle 2.2.1.2. Il est recommandé que, pour tout personnel non permanent devant accéder à une application ou un équipement sensible du SI, un tutorat par une personne de la structure soit mis en place, afin de l'informer des règles SSI et de s'assurer de leur application (sans toutefois que cette personne ne porte la responsabilité du respect des règles par le personnel non permanente).	
2.2.2.3	La procédure de prise de fonction lors d'un mouvement interne devrait intégrer les étapes sécurité suivantes : • le cas échéant, restitution et/ou remise de matériel informatique et signature du registre de prise en charge de matériel ; • le cas échéant, restitution et/ou remise de moyen(s) d'authentification lié à la/aux fonction(s) (ex. CDE) et des consignes d'utilisation. (ex. notice explicative relative aux conditions générales d'utilisation des cartes de la famille CPx accessible sur le site esante.gouv.fr) ; • le cas échéant, restitution ou changement de paramétrage de moyen(s) d'accès aux locaux et aux coffres, armoires… ; • rappel des règles de gestion des mots de passe et de la sécurité des postes de travail telles que présentées dans les thèmes 4-5.1 et 4-5.2 ; • rappel des contacts sécurité en cas d'incident ; • détermination du/des profil(s) utilisateur(s) correspondant à la/aux fonction(s) prise(s) tel que présenté dans le thème 5-1.1 ; • le cas échéant, suppression des droits d'accès précédemment détenus et ne correspondant plus au profil(s) utilisateur(s) identifié(s) ; • attribution des droits d'accès correspondant au profil(s) utilisateur(s) identifié(s) ; • le cas échéant, désactivation de comptes si les conditions d'attribution de plusieurs comptes présentées dans la règle 5.2.1.4 ne sont plus remplies suite au mouvement interne ;	*Catégorie de personne*

[7] Voir règle 5.2.1.4 sur les conditions d'attribution de plusieurs comptes à un utilisateur.

	• le cas échéant, changement des mots de passe dont l'utilisateur avait connaissance et permettant l'accès à des composants du SI auxquels il ne doit plus accéder désormais.	
2.2.2.4	La procédure de départ (que ce soit définitif ou pour mouvement interne) devrait intégrer les étapes sécurité suivantes : • le cas échéant, restitution du matériel informatique mis à disposition et signature du registre de remise de matériel ; • le cas échéant, restitution des moyen(s) d'authentification lié à la/aux fonction(s) (ex. CDE) ; • le cas échéant, restitution des moyen(s) d'accès aux locaux et aux coffres, armoires… (clés, cartes, …) ; • résiliation des droits d'accès correspondant au/aux profil(s) utilisateur(s) ; • en cas de départ de la structure, désactivation du/des compte(s) nominatif(s) du partant, • le cas échéant, changement des mots de passe dont l'utilisateur avait connaissance et permettant l'accès à des composants du SI (notamment : mots de passe d'administration d'équipements, mots de passe « partagés » s'il en existe de manière dérogatoire…).	*Catégorie de personnel*
2.2.2.5	Toute dérogation à une règle de la PSSI ne peut être autorisée qu'après validation par le Responsable de la SSI et par le responsable du SI concerné. Les dérogations doivent être données pour une durée limitée, fixée au cas par cas (ex. dérogation temporaire de quelques mois, ou dérogation « permanente » due à un manque fonctionnel dans une application, qui ne pourra être levée que lorsque l'éditeur de l'application aura apporté les modifications nécessaires). Elles doivent être consignées dans un ticket.	*Catégorie de personnel*
2.2.2.6	Les dérogations aux règles de la PSSI devraient faire l'objet d'une revue annuelle par les personnes indiquées au 2.2.2.5 pour confirmer ou non leur maintien.	*Catégorie de personnel*
2.2.2.7	Les procédures de gestion de la SSI et les procédures « sensibles » de gestion du SI en général (i.e. celles qui sont susceptible d'avoir un impact sur la sécurité du SI) doivent être établies conjointement par le service informatique et le Responsable de la SSI. Elles doivent intégrer les étapes de validation des points clés de la procédure par le Responsable de la SSI ou par un responsable approprié chaque fois que les enjeux SSI liés à la procédure le justifient.	*Catégorie de personnel*

Thématique 3 : Assurer la sécurité physique des équipements informatiques du SI

T3-1 Maîtriser l'accès aux équipements du SI qui sont nécessaires à l'activité de la structure et assurer leur protection physique

T3-1.1 Assurer la protection physique des équipements informatiques d'infrastructure (serveurs, réseau) du SI qui contiennent des données sensibles (dont les données de santé à caractère personnel)

Une protection physique adéquate des équipements informatiques d'infrastructure est indispensable pour limiter les risques de dommages, accidentels ou malveillants, ou de vol de ces équipements, situations qui entraineraient à minima une interruption du service.

De plus, l'accès physique d'une personne malveillante à un équipement informatique peut lui permettre de disposer d'un accès privilégié à cet équipement (obtention du mot de passe administrateur, modification des logiciels, accès illégitime à des données sensibles[8], …) à l'insu de ses exploitants légitimes.

Exigences :

⇒ Tout équipement informatique d'infrastructure qui participe au traitement (stockage, transmission réseau, …) de données sensibles (données de santé à caractère personnel, autres données à caractère personnel, autres données sensibles…) ou à la sécurité d'équipements qui y participent (serveur d'authentification, pare-feu, …) doit être hébergé dans un local ou une enceinte dont l'accès est contrôlé et dont la protection des ouvertures est renforcée.

⇒ L'accès aux locaux ou enceintes qui hébergent les équipements informatiques d'infrastructure doit être limité aux seules personnes autorisées.

⇒ Quand les risques le justifient (sensibilité des données stockées, valeur des équipements, … mis en regard de l'environnement d'hébergement), un dispositif d'alarme, voire de vidéo-surveillance, doit être mis en place.

⇒ Les locaux qui hébergent les équipements informatiques d'infrastructure doivent être choisis et aménagés de telle sorte qu'ils garantissent l'ensemble des conditions nécessaires au bon fonctionnement des équipements.

Déclinaison en règles :

Règles sur la protection physique des équipements d'infrastructure du SI :

Réf.	Règles	Catégories de moyens du SI concernées
3.1.1.1	Les dispositifs qui participent au traitement de données sensibles : • serveurs ; • systèmes de stockage de données ; • systèmes de sauvegarde ; ou qui fournissent les infrastructures réseau et sécurité utilisées par ces dispositifs : • routeurs, commutateurs, hubs, … • pare-feux, proxies, passerelles antivirus…	*Tout équipement du SI*

[8] Données de santé à caractère personnel, données à caractère personnel, toutes autres données jugées sensibles dans le cadre d'une analyse de risque.

	• serveur de sécurité (authentification…) • serveurs DHCP, DNS, … ou qui fournissent des services techniques nécessaires au bon fonctionnement et à la sécurité du SI : • baies de brassage réseau ou téléphonique ; • système téléphonique (autocommutateur, système de taxation..,) ; • éléments clés de l'infrastructure électrique : armoires électriques, onduleurs et batteries associées, générateur électrique de secours… • système de climatisation de la salle informatique ; • système de gestion technique centralisée (GTC) ou de gestion technique de bâtiment (GTB) ; • centrale d'alarme et de lutte anti-incendie ; • système de détection d'inondation dans les locaux informatiques ; • système de contrôle d'accès aux bâtiments ; • centrale d'alarme anti-intrusion, • système de vidéo-surveillance… sont hébergés : • soit dans des locaux dont l'accès est sécurisé (dénommés « locaux sécurisés » par la suite) ; • soit dans des baies informatiques dont l'accès est sécurisé (dénommées « baies sécurisées » par la suite).	
3.1.1.2	La sécurisation de l'accès à un local sécurisé doit s'appuyer sur : • le choix d'un local présentant le moins d'ouvertures possibles sur l'extérieur ; • la mise en place de barreaux aux fenêtres et selon la localisation de la salle (cas notamment des salles en rez-de-chaussée avec fenêtre sur lieu public), l'utilisation de grilles de protection ou de verre renforcé contre les projectiles (pierres, …); • la mise en œuvre d'un contrôle d'accès au local adapté à la fréquence des interventions du personnel (par exemple, fermeture par clé des locaux techniques d'étage, porte à lecteur de badge, ou à défaut à code, pour le local informatique plus fréquemment visité) ; • la mise en place d'alarme, voire d'enregistreur vidéo, selon les enjeux identifiés par l'analyse de risque.	*Locaux d'hébergement du SI*
3.1.1.3	La sécurisation d'une baie sécurisée doit s'appuyer sur : • l'utilisation d'une baie informatique (ou adaptée au type d'équipement protégé quand ce n'est pas un équipement informatique) professionnelle pouvant être intégralement fermée et pouvant être ouverte en face avant comme en face arrière ; • l'intégration dans la même baie de tout écran, clavier, souris ou autre périphérique type ILO	*Locaux d'hébergement du SI*

	nécessaire à l'administration des équipements à sécuriser ; • la mise en œuvre d'un système de fermeture commandé par lecteur de badge, ou à défaut à code ou à clé ; • si la baie est assez légère pour être volée, une fixation fiable de la baie au mur ou au sol ; • la mise en place d'alarme, recommandée, voire d'enregistreur vidéo, selon les enjeux identifiés par l'analyse des risques.	
3.1.1.4	Une gestion stricte des personnes autorisées à accéder à chaque local et baie sécurisés devrait être organisée : • la liste des personnes autorisées doit être établie, maintenue à jour et validée par les responsables des traitements concernés ; Elle doit être revue au minimum une fois par an ; • les moyens d'accès utilisés doivent être contrôlés (attribution nominative des clés, des codes de porte) et gérés (renouvellement au moins semestriel des codes, ainsi que lors de sortie de personnels de la liste des personnes autorisées) ; • une procédure pour l'accès accompagné et ponctuel de personnes sans autorisation permanente (prestataire externe, personnel des services généraux…) doit être établie ; • un registre des accès effectués par des personnes sans autorisation permanente devraitt être tenu et intégré à la procédure mentionnée ci-dessus. Doivent y être consignées la date et l'heure de début et de fin de la visite, l'identité du visiteur, l'identité de l'accompagnant et l'objet de la visite. Les entrées de ce registre devraient être conservées 1 an.	*Locaux d'hébergement du SI*
3.1.1.5	Tout local sécurisé, et tout local qui héberge une baie sécurisée, devrait être choisi ou aménagé pour respecter les conditions nécessaires au bon fonctionnement des équipements : • température (par aération et/ou mise en œuvre d'un système de climatisation adapté à la dissipation thermique des équipements hébergés); • hygrométrie ; • absence de stockage de carton, papier, ou autre source potentielle de départ de feu ; • absence de poussière excessive ; • absence de risque particulier d'inondation ou d'incendie qui serait induit par le passage de conduites ou aggravé par la proximité avec d'autres locaux qui présentent ces risques ; • absence de rayonnements électromagnétiques provoqués par la proximité de machines électriques puissantes ou de certains équipements médicaux (ou protection spécifique contre ces rayonnements).	*Locaux d'hébergement du SI*

3.1.1.6	Tout local sécurisé, et tout local qui héberge une baie sécurisée, doit disposer d'une alimentation électrique : • aux normes en ce qui concerne la protection des personnes et des équipements ; • de capacité suffisante au regard des équipements connectés ; Un inventaire des consommations doit être maintenu et vérifié avant ajout ou remplacement d'équipement ; • régulée et protégée contre les surtensions ; Un soin particulier doit être apporté à ce point dans les zones géographiques où les orages sont fréquents ; • maintenue en cas de coupure de l'alimentation secteur à l'aide d'onduleurs, voire de générateur électrique, au minimum le temps nécessaire à l'arrêt des équipements (qui devrait être automatisé), voire plus selon les exigences de disponibilité des systèmes hébergés. Le bon fonctionnement de ces équipements de secours et de leur activation en cas de coupure de l'alimentation secteur doit être vérifié régulièrement et donner lieu à un suivi formalisé.	*Locaux d'hébergement du SI*
3.1.1.7	Dans la mesure du possible, l'alimentation électrique secourue doit être constituée d'au moins un circuit électrique spécifique, distinct de celui éventuellement utilisé pour les postes de travail et sur lequel n'est connecté aucun équipement non informatique fortement consommateur (radiateur électrique, bouilloire…) ou susceptible de provoquer des perturbations électriques. Le personnel devrait être sensibilisé au fait que de tels équipements ne doivent pas être branchés sur le circuit électrique régulé et secouru, quand ce circuit est disponible.	*Locaux d'hébergement du SI*
3.1.1.8	Tout local sécurisé, et tout local qui héberge une baie sécurisée, qui accueille des dispositifs mentionnés au 3.1.1.1, doit disposer d'un système de lutte anti-incendie conforme aux normes en vigueur : • détection d'incendie ; • protection des personnes, évacuation du local (nécessité que le personnel puisse évacuer la salle en toute circonstance malgré le dispositif de contrôle d'accès à la salle), masques respiratoires en cas de système d'extinction automatiques par gaz, … • dispositifs d'extinction adaptés, …	*Locaux d'hébergement du SI*
3.1.1.9	Des procédures de réaction doivent être établies et communiquées au personnel concerné pour les situations d'incident qui toucheraient un local ou une baie sécurisés : • incendie ; • coupure d'alimentation électrique ; • défaillance du dispositif de contrôle d'accès au local ou à la baie ; • panne de climatisation ou hausse excessive de température de du local ;	*Locaux d'hébergement du SI*

	• intrusion dans les locaux ; • inondation.	

T3-1.2 Assurer la protection physique des postes de travail qui contiennent des données sensibles (dont les données de santé à caractère personnel)

Les postes de travail qui permettent l'accès à des données de santé à caractère personnel ou à d'autres données sensibles, voire qui stockent de telles données, doivent être protégés afin d'éviter qu'une personne non autorisée puisse accéder à ces informations sensibles.

Exigences :

⇒ Les postes de travail doivent, autant que possible, être situés hors d'atteinte des personnes non autorisées et en particulier du public (usagers, accompagnant) ;
⇒ Les écrans des postes de travail ne doivent être visibles que par leur utilisateur ;
⇒ Les postes de travail facilement transportables (ordinateurs portables, tablettes, …) doivent être protégés contre le vol ;
⇒ Si un poste de travail assure le stockage de données, le local qui l'héberge doit être choisi et aménagé de telle sorte qu'il garantisse l'ensemble des conditions nécessaires au bon fonctionnement du poste. Pour les autres postes de travail, cette exigence peut être prise comme recommandation.
⇒ De manière générale, les locaux qui hébergent des postes de travail ne doivent pas présenter de risque particulier du point de vue de l'environnement de travail.

Déclinaison en règles :

Règles sur la protection physique des postes de travail :

Réf.	Règles	Catégories de moyens du SI concernées
3.1.2.1	Les postes de travail devraient, autant que possible, être situés hors de la zone de circulation du public. Dans tous les cas, ils doivent être positionnés afin d'interdire un accès direct au poste par le public (usager, accompagnant…).	*Équipements utilisateurs/Terminaux (ex. Postes de travail fixes standard)*
3.1.2.2	Les écrans des postes de travail devraient être orientés de telle sorte que les personnes non autorisées ne puissent pas lire ce qu'ils affichent. Les possibilités de visibilité depuis l'arrière de l'utilisateur (fenêtres, cloisons transparentes,…) doivent être prises en compte. Si nécessaire, des filtres installables sur l'écran devraient être mis en place afin d'en réduire l'angle de visibilité. Ces règles, auxquelles les utilisateurs concernés doivent être sensibilisés, s'appliquent également aux postes nomades (ordinateurs portables, tablettes…) autorisés à stocker des données sensibles.	*Équipements utilisateurs/Terminaux*
3.1.2.3	Les ordinateurs portables ou suffisamment peu volumineux pour être facilement transportés, ainsi que les autres terminaux légers (tablettes) devraient être attachés à un point fixe ou lourd (bureau) (par exemple par un câble antivol) en l'absence de leur utilisateur. Il doit être pris soin de choisir un point d'accroche fiable, duquel l'attache ne peut être retirée simplement.	*Équipements utilisateurs/Terminaux*

	A défaut, ils doivent être systématiquement rangés dans un placard ou un coffre, fermé à clé en l'absence de leur utilisateur.	
3.1.2.4	Un câble antivol devrait être fourni conjointement à tout ordinateur portable confié à un utilisateur. L'utilisateur doit être sensibilisé à son utilisation.	*Équipements utilisateurs/Terminaux*
3.1.2.5	Les postes de travail doivent disposer d'une alimentation électrique : • aux normes en ce qui concerne la protection des personnes et des équipements ; • de capacité suffisante au regard des équipements connectés. Un inventaire des consommations doit être maintenu et vérifié avant ajout ou remplacement d'équipement sur le même circuit ; • régulée et protégée contre les surtensions ; un soin particulier doit être apporté à ce point dans les zones géographiques où les orages sont fréquents ; Les postes de travail devraient disposer d'une alimentation électrique : • maintenue en cas de coupure de l'alimentation secteur à l'aide d'onduleurs voire de générateur électrique, au minimum le temps nécessaire à l'arrêt des postes, voire plus selon les exigences de disponibilité de l'activité.	*Locaux donnant accès au SI*
3.1.2.6	Dans la mesure du possible, les postes de travail doivent être alimentés par un circuit électrique spécifique et sur lequel n'est connecté aucun équipement fortement consommateur (radiateur électrique, bouilloire…) ou susceptible de provoquer des perturbations électriques. De tels équipements ne doivent pas être branchés sur le circuit électrique régulé et secouru, quand ce circuit est disponible.	*Locaux donnant accès au SI*
3.1.2.7	Les locaux qui hébergent les postes de travail ne devraient pas présenter de risque particulier du point de vue de l'environnement de travail, qu'il s'agisse de risque de dégâts des eaux, d'incendie ou de pollution, découlant de leur propre configuration ou de la proximité d'autres locaux qui présenteraient ces risques.	*Locaux donnant accès au SI*

T3-1.3 Assurer la protection physique des équipements amovibles qui contiennent des données sensibles (dont les données de santé à caractère personnel)

Les supports de données amovibles, du fait de leur facilité de transport, sont particulièrement susceptibles d'être égarés ou volés.

Exigences :

⇒ Les supports de données amovibles doivent être protégés contre le vol.

⇒ Les utilisateurs doivent être particulièrement sensibilisés à la protection de ce type de support.

Déclinaison en règles :

Règles sur la protection physique des équipements amovibles, qui contiennent des données de santé à caractère personnel ou d'autres données sensibles :

Réf.	Règles	Catégories de moyens du SI concernées
3.1.3.1	En l'absence de son utilisateur, tout support amovible (disque dur externe, clé USB, CD, DVD) de données de santé à caractère personnel, ou plus généralement de données sensibles, devrait être rangé dans un placard ou coffre fermé à clé (ou à code).	*Équipements utilisateurs/Supports de données amovibles*
3.1.3.2	Il est recommandé de ranger tout support amovible (disque dur externe, clé USB, CD, DVD) de données de santé à caractère personnel, ou plus généralement de données sensibles, dès lors qu'il n'est plus utilisé.	*Équipements utilisateurs/Supports de données amovibles*

T3-1.4 Assurer la destruction de données lors du transfert de matériels informatiques

L'activité des SI de santé conduit à stocker des données sensibles sur différents supports informatiques (ex : disques durs, bandes magnétiques, clés USB, CD, DVD ...).

Le cycle de vie des matériels (réaffectation d'un matériel en interne, envoi d'un matériel en maintenance, mise au rebut du matériel, …) peut conduire un tiers à accéder à ces matériels et, de là, à accéder de façon indue aux données qu'il contient. C'est de ce risque d'accès illégitime d'un tiers aux données contenues dans l'équipement qu'il est nécessaire de se protéger.

On distingue :

- le transfert (ou recyclage) interne de matériel, au sein de la même structure (avec changement d'utilisateur)
- le transfert externe, par exemple:
  - la sortie temporaire du matériel (par exemple dans le cadre d'une opération de maintenance ou de garantie) ;
  - la cession du matériel ou son retour au fournisseur en fin de location ;
  - la mise au rebut du matériel : destruction de matériel, par exemple en raison d'un dysfonctionnement le rendant impropre à l'usage ou en cas de fin de vie, supports de sauvegardes usés…

Exigences :

⇒ Une procédure formalisée doit être mise en place, qui garantisse que tout matériel informatique faisant l'objet d'un transfert voit l'ensemble des données qu'il contient effacées par une méthode adéquate.

⇒ La méthode d'effacement utilisée doit être choisie en fonction du type de transfert (interne ou externe), de la nature de l'équipement et de la sensibilité des données concernées, afin d'assurer un effacement efficace pour réduire le risque de fuite de données à un niveau acceptable.

Déclinaison en règles :

Règles générales sur la destruction de données lors du transfert de matériels informatiques :

Réf.	Règles	Catégories de moyens du SI concernées
3.1.4.1	La destruction de données doit être réalisée sous la responsabilité du responsable du SI, soit par le personnel de la structure soit par des prestataires techniques externes dans le cadre de contrats.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.2	Afin de définir les responsabilités des acteurs impliqués dans le processus de destruction de données, les règles de ce guide devraient être reprises dans les documents propres à l'organisation du SI (politique de sécurité, charte informatique, notes d'organisation, fiches de poste, contrats d'externalisation, …). A titre d'exemple, les utilisateurs de supports de stockage amovibles sont chargés de l'application des règles d'effacement lors du transfert de matériels, conformément à la charte informatique de la structure.	*Catégorie de personnel (ex. Responsable de la SSI, Responsable du SI)*
3.1.4.3	Les interventions techniques doivent être réalisées selon le type de matériel considéré. Dans le cas d'un équipement (ordinateur portable ou fixe, serveur, photocopieur, ordiphone …) comportant plusieurs composants (disque dur, clé USB, carte SD, …), chaque composant devra être traité indépendamment selon les règles applicables.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.4	Les procédures de destruction de données lors du transfert de matériel informatique devraient être formalisées.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.5	Les procédures de gestion du cycle de vie des supports de données numériques devraient être formalisées et intégrer le traitement des données et leur destruction.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.6	Avant toute opération d'effacement ou de destruction, il est préconisé de contrôler que les supports ne contiennent aucune donnée utile et non sauvegardée par ailleurs. Dans le cas contraire, il convient de procéder à la sauvegarde des données qui sont nécessaires.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.7	Une fois l'effacement terminé, Il est nécessaire de vérifier que le support ne contient plus de données.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.8	Une fiche d'intervention à destination du responsable de la gestion des matériels, visée par le personnel en charge de l'opération, devrait permettre de garder une trace des informations suivantes pour les matériels du SI : • Identification du matériel (numéro de série, adresse MAC …)	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

	• ancien propriétaire (entité, ou à défaut identité personne physique) ; • nouveau propriétaire (entité, identité personne physique) ; • date de transfert de l'équipement ; • date et nature de l'intervention d'effacement ou de destruction effectuée; • statut des opérations réalisées (opérateur, date, type d'effacement, contrôle de l'effacement, …)	
3.1.4.9	Les procédures de traitement du matériel en fin de vie, notamment quand elles impliquent un transfert externe du matériel, devraient prévoir la gestion des supports de données numériques qui peuvent être contenus dans ces matériels.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

Règles techniques sur la destruction de données, spécifiques aux disques durs et aux supports flash (clé USB, carte SD, Compact Flash, …) :

Réf.	Règles	Catégories de moyens du SI concernées
3.1.4.10	Dans le cas d'un recyclage interne uniquement, un formatage complet devrait être réalisé. Ce formatage complet (dit aussi formatage bas niveau ou à zéro[9]) devrait être appliqué sur la totalité de la ou des partitions du support considéré.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.11	Dans les autres cas, un effacement renforcé devrait être réalisé avec un logiciel utilisant l'algorithme conforme au «NISP Operating Manual (DOD 5220.22-M) », de préférence un produit labellisé par l'ANSSI (voir règle 6.5.1.9). Cet effacement devrait être appliqué sur la totalité de la ou des partitions du support considéré. La complexité de l'effacement sera de : • 3 passes minimum pour les supports du type disque dur • 1 passe pour les supports flash	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.12	Il est envisageable, en alternative à la règle 3.1.4.11, de procéder : • à la démagnétisation des disques durs, ou à leur destruction physique (broyage, incinération …) ; • à la destruction physique des supports flash (broyage ou incinération).	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

[9] Dans un formatage à zéro, chaque bit de donnée est remplacé par un zéro. Remarque : la simple réinstallation du système n'est pas suffisante pour assurer la destruction des données.

Règles techniques sur la destruction de données pour d'autres types de supports de données:

Réf.	Règles	Catégories de moyens du SI concernées
3.1.4.13	Les disques optiques devraient être détruits par destruction physique (broyage, incinération ou meulage).	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.14	Les cartes à microcircuits (carte SIM, CPS, …) devraient être détruites par broyage du circuit ou incinération.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.15	Les données stockées sur des ordiphones (« smartphones »), téléphones portables et tablettes devraient être effacées à l'aide des fonctions d'utilisation puis par application de la procédure prévue par le constructeur pour remise de l'appareil en configuration de sortie d'usine.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
3.1.4.16	Les données des matériels stockant des informations sur des supports autres que ceux-spécifiés ci-dessus (par exemple, dispositifs biomédicaux, …) devraient être effacées à l'aide des fonctions d'utilisation puis par application de la procédure prévue par le constructeur pour remise de l'appareil en configuration de sortie d'usine.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

Thématique 4 : Protéger les infrastructures informatiques

T4-1 Maîtriser le parc informatique

T4-1.1 Identifier physiquement chaque équipement informatique (serveurs, poste de travail, équipement réseau, …) ou dispositif médical connecté détenu par la structure

Exigence :

⇒ Tout équipement informatique, connecté ou non au réseau du SI et tout dispositif médical connecté au SI, détenu par la structure, doit être identifié et recensé dans l'inventaire des composants du SI avec les informations utiles à sa gestion.

Déclinaison en règles :

Règles sur l'identification des équipements informatiques :

Réf.	Règles	Catégories de moyens du SI concernées
4.1.1.1	Un inventaire doit être établi et comprendre : - l'ensemble des équipements informatiques (serveurs, équipements réseau, postes de travail, tablettes, ordiphones/smartphones, imprimantes, modems, téléphones IP et tout autre dispositif connecté au réseau : fax, système téléphonique, système de visioconférence, webcams/caméras vidéo, lecteur de badges, systèmes d'alarme, dispositifs de gestion technique de bâtiment…) ; - les dispositifs médicaux détenus par la structure. L'inventaire devrait inclure les équipements appartenant à la structure, ainsi que ceux qui lui sont loués ou prêtés. L'utilisation d'un outil d'inventaire du SI facilite l'élaboration, la maintenance et l'exploitation de l'inventaire.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.1.2	Un identifiant numérique unique doit être attribué à chaque équipement inventorié.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.1.3	Chaque équipement doit être marqué avec une étiquette reconnaissable (pour la distinguer d'autres étiquettes éventuellement présentes, par exemple par indication du nom ou logo de la structure) qui comporte l'identifiant attribué à l'équipement dans l'inventaire sous forme alphanumérique et sous forme de code barre (ou de code barre 2D) pour faciliter les opérations d'inventaire.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.1.4	Pour chaque équipement, l'inventaire doit également enregistrer au minimum les informations suivantes : • Identifiant • Désignation • Catégorie d'équipement • Fournisseur	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

	• Référence du modèle • Caractéristiques principales • Localisation • Utilisateur ou responsable de l'équipement • Type de détention : propriété, location, prêt • Propriétaire de l'équipement • Supports de données présents dans l'équipement (ex. aucun / intégré et inamovible / 2 disques durs / 1 disque dur SSD…)	
4.1.1.5	L'inventaire doit être mis à jour pour tout début ou fin de détention d'équipement qui entre dans le périmètre de l'inventaire. L'étiquetage doit être réalisé conjointement à cette mise à jour.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.1.6	Une procédure doit définir les modalités d'enregistrement et de gestion des demandes de matériel formulées par les utilisateurs, et de suivi du cycle de vie de ce matériel quel qu'il soit, et les décliner si nécessaire selon le type de matériel (poste de travail, téléphone mobile, poste de travail fixe ou portable, équipement biomédical, clé USB, …). Cette procédure doit faire le lien avec les sujets traités dans la Thématique 6, et intégrer les phases de remise du matériel à l'utilisateur et de restitution du matériel.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.1.7	Seuls les équipements fournis par le service informatique de la structure, ou validés par lui dans le cas d'équipements entrant dans le cadre de la prestation d'un tiers, doivent être intégrés au SI. La mise en œuvre d'équipements de type ou de modèle nouveau doit être soumis à la validation du Responsable de la SSI, et si nécessaire donner lieu à une analyse de risque.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T4-1.2 Identifier les composants logiciels du SI

Pour les mêmes raisons que celles relatives aux composants matériels du SI, les composants logiciels du SI doivent être recensés.

Exigence :

⇒ Tout système d'exploitation ou logiciel applicatif installé sur un équipement présent dans l'inventaire des équipements informatique du SI doit être identifié et recensé dans l'inventaire des composants logiciels du SI avec les informations utiles à sa gestion.

Déclinaison en règles :

Règles sur l'identification des composants logiciels :

Réf.	Règles	Catégories de moyens du SI concernées
4.1.2.1	Il doit être établi un inventaire de tout système d'exploitation et de toute application installés sur les équipements référencés dans l'inventaire des équipements informatiques. La granularité retenue pour cet inventaire est : • celle des ensembles logiciels dont le service informatique gère unitairement l'installation et le maintien à jour ; • celle de l'équipement lui-même quand il s'agit d'un logiciel embarqué et intégré qui assure l'essentiel des fonctions de l'équipement. A titre d'exemples d'ensembles logiciels qui peuvent être considérés unitairement, on peut citer : • le système d'exploitation d'un poste de travail ou d'un serveur et les éventuelles applications installées par défaut avec lui ; • la suite bureautique dans son ensemble, même si celle-ci intègre plusieurs applications différentes ; • le logiciel anti-virus du poste de travail ; • le système de base de données et l'application à laquelle il est dédié ; • le système de base de données lui-même, s'il est utilisé de manière indépendante par plusieurs applications ; • l'ensemble logiciel d'un équipement médical connecté ; • l'ensemble logiciel d'un téléphone IP, ou d'une imprimante.	*Equipements d'infrastructure système et réseau/Logiciel, Equipements utilisateurs/Logiciel*
4.1.2.2	Pour chaque entrée de l'inventaire des logiciels, les informations suivantes (au minimum) devraient également être renseignées : • Désignation • Catégorie de logiciel • Fournisseur • Applications ou composants principaux • Caractéristiques principales • Responsable du logiciel	*Equipements d'infrastructure système et réseau/Logiciel, Equipements utilisateurs/Logiciel*

	• Type de détention : propriété, location, prêt • Propriétaire du logiciel • Version • Niveau de support assuré par l'éditeur • Licence : nombre d'utilisateur, de postes, processeurs, … autorisés • Date de fin de validité de la licence • Liste des identifiants d'équipements sur lesquels l'ensemble logiciel est installé Cet inventaire peut également être le bon support pour noter et suivre la date de dernière vérification de disponibilité de mise à jour pour chaque logiciel.	
4.1.2.3	Une procédure devrait définir les modalités d'enregistrement et de gestion des demandes de logiciel formulées par les utilisateurs. Cette procédure doit faire le lien avec les sujets traités dans la Thématique 6,	*Equipements d'infrastructure système et réseau/Logiciel, Equipements utilisateurs/Logiciel*
4.1.2.4	Seuls les logiciels fournis par le service informatique de la structure doivent être intégrés au SI. La mise en œuvre de logiciels de type ou de modèle nouveau doit être soumis à la validation du Responsable de la SSI, et si nécessaire donner lieu à une analyse de risque.	*Equipements d'infrastructure système et réseau/Logiciel, Equipements utilisateurs/Logiciel*

T4-1.3 Identifier les services d'infrastructure du SI

Il est essentiel que les services d'infrastructure soient identifiés et documentés, que ce soit pour en faciliter la gestion au quotidien, intervenir efficacement en cas d'incident, identifier les éventuels défauts de conception dans le cadre d'une revue ou préparer et déployer les évolutions du SI et de son infrastructure.

Exigence :

⇒ L'ensemble des services d'infrastructure du SI, aux niveaux physique et logique, doit être documenté.

Déclinaison en règles :

Règles sur l'identification des services d'infrastructure du SI :

Réf.	Règles	Catégories de moyens du SI concernées
4.1.3.1	Les services techniques nécessaires au bon fonctionnement et à la sécurité du SI devraient être identifiés et documentés : • Alimentation électrique des équipements informatiques ; • Climatisation des locaux informatiques ; • Dispositifs anti-incendie des locaux informatiques ; • Moyens de télécommunications externes (lignes ou liens d'accès aux réseaux téléphoniques, liens d'accès Internet, liaisons de télécommunications spécifiques filaires, radio, laser ou satellitaires…) ; • Infrastructure de câblage téléphonique ; • Infrastructure de contrôle d'accès et d'alarme des locaux informatiques.	*Equipements d'infrastructure système et réseau, Locaux d'hébergement du SI*
4.1.3.2	Les services informatiques d'infrastructure nécessaires au bon fonctionnement et à la sécurité du SI devrait être identifiés et documentés : • Infrastructure réseau physique : câblage, équipements réseau (routeurs, commutateurs, hubs, ponts, points d'accès Wifi et zones de couverture associées…) ; • Infrastructure réseau logique : plan d'adressage, routage, VLAN, pare-feux, passerelles ; • Services d'infrastructure réseau : DHCP, DNS, NTP… • Services de sécurité : services d'authentification, service de domaine, détection d'intrusion réseau, passerelles anti-virus, service d'enregistrement et de gestion de traces, annuaires utilisateurs utilisés pour le contrôle d'accès, services liés à la mise en œuvre de certificats électroniques, service de sauvegarde, services d'administration des services de sécurité… • Services de téléphonie IP ; • Services d'administration du SI.	*Equipements d'infrastructure système et réseau*

T4-1.4 Vérifier régulièrement la complétude de ce recensement et vérifier l'existence des licences nécessaires

Les inventaires des équipements, des logiciels et de services d'infrastructure ne sont utiles que s'ils sont maintenus à jour. La vérification régulière de leur complétude permet d'une part de combler les manques dans les inventaires et d'autre part d'identifier les éléments présents de manière illégitime dans le SI.

Exigences :

⇒ Les inventaires et les informations associées doivent être maintenus à jour au fil des ajouts, retraits et modifications des éléments qu'ils recensent.

⇒ Une revue régulière, au moins annuelle, de ces inventaires doit être organisée afin d'identifier et de traiter les écarts entre inventaire enregistré et parc informatique constaté.

⇒ Cette revue doit également être l'occasion de vérifier que la structure est en règle vis-à-vis des licences dont elle dispose au regard des logiciels effectivement déployés sur les différents équipements.

Déclinaison en règles :

Règles sur la vérification régulière des inventaires :

Réf.	Règles	Catégories de moyens du SI concernées
4.1.4.1	Les procédures de gestion du parc informatique devraient prévoir la mise à jour de l'inventaire et des informations associées à l'occasion de toute entrée ou sortie du parc informatique, quel que soit le statut de l'élément concerné (en propriété ou non de la structure).	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.4.2	Une opération annuelle d'inventaire des composants du parc informatique, matériels comme logiciels, effectivement déployés ou stockés devrait être organisée. Il est recommandé que soient mis en œuvre des outils de vérification automatique de la conformité des configurations effectives (notamment celles des postes de travail, voire des serveurs) avec les configurations prévues dans le cadre de la règle 4.5.3.13. Cette automatisation, permet, outre un allègement de la charge de travail du personnel informatique, une vérification fréquente de la conformité des configurations et une détection précoce des dérives et autres anomalies.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.4.3	Lorsque l'inventaire annuel fait apparaitre des disparitions au regard de l'inventaire attendu, une investigation devrait être menée pour chaque élément manquant afin, au-delà du recouvrement des biens, d'en identifier les éventuels impacts sur la sécurité du SI. En particulier, il doit être déterminé si les éléments manquants participaient à la sécurité du SI, ou s'ils étaient susceptible de stocker des informations à caractère personnel, auquel cas le processus de gestion des évènements de sécurité doit être activé.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

4.1.4.4	Lorsque l'inventaire annuel fait apparaitre des éléments imprévus au regard de l'inventaire attendu, une investigation devrait être menée pour chaque élément concerné afin d'en identifier l'origine et les éventuels impacts sur la sécurité du SI. Il doit être porté un soin particulier à la détection des logiciels et équipements (borne Wifi, modem, composant USB inconnu rajouté sur le branchement du clavier...) installés illégitimement et susceptibles de permettre des communications non maîtrisées ou des atteintes à la sécurité du SI. Le processus de gestion des évènements de sécurité devrait être activé dans ce type de situation. Une autre raison pour laquelle la détection de bornes Wifi illégitimes est indispensable est que ces bornes sont disposées sans étude préalable de localisation ni de puissance. Elles sont de ce fait susceptibles de perturber les équipements médicaux, voire de porter atteinte à la santé des usagers.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.1.4.5	Outre l'inventaire annuel, une opération de recherche devrait être menée au moins semestriellement afin de détecter les logiciels et équipements non gérés par le responsable du SI et susceptibles de porter atteinte à la sécurité du SI, tels que : • Logiciels destinés à l'intrusion dans les SI ou à la recherche de mots de passe ; • Logiciels destinés à établir des tunnels de communication avec l'extérieur ou de manière générale à contourner les dispositifs de sécurité du SI ; • Logiciels cryptographiques (chiffrement…) ; • Logiciels de communication instantanée ou d'échange de données ; • Bornes Wifi ; • Adaptateurs Wifi ou Bluetooth sur port USB ; • Modems ; • Tout composant inconnu connecté à un port USB ou rajouté au branchement du clavier. Le processus de gestion des évènements de sécurité devrait être activé en cas de détection. La détection des logiciels illégitimes peut être réalisée, par exemple, à l'aide d'un logiciel centralisé d'inventaire logiciel, qui peut également identifier automatiquement les logiciels potentiellement néfastes. La détection des adaptateurs Wifi sur USB et des modems illégitimes peut être réalisée à l'aide d'un logiciel centralisé qui examine la configuration des périphériques de chaque équipement. Certains logiciels utilisables pour détecter les logiciels illégitimes disposent aussi de cette fonction. L'utilisation temporaire d'adaptateur Wifi peut parfois être détectée	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

	par ce moyen, même si l'adaptateur n'est plus connecté au moment du contrôle. Les mesures de détection des périphériques illégitimes, l'identification/authentification des équipements connectés au SI et la recherche de flux anormaux sur le réseau constituent un premier niveau pour détecter ou interdire la mise en place d'accès Wifi illégitimes. La détection et la localisation de bornes Wifi illégitimes peut être effectuée avec la meilleure fiabilité en utilisant des dispositifs qui s'appuient sur la détection radio de ces bornes, que ce soit à l'aide d'un équipement dédié, ou d'un logiciel spécifique installé sur un portable standard disposant d'une carte Wifi (ce sont souvent les mêmes outils que ceux utilisés pour choisir le bon positionnement des bornes légitimes). Il convient de souligner que des points d'accès Wifi peuvent très bien être détectés dans une structure sans que la sécurité du SI soit impactée. C'est notamment le cas de structure qui accueillent du public, où certains visiteurs non malveillants peuvent avoir activé le mode « point d'accès Wifi » sur leur téléphone mobile. Cette innocuité envers le SI n'enlève toutefois rien aux risques de perturbation des équipements médicaux.	
4.1.4.6	L'inventaire annuel devrait comptabiliser les utilisations qui sont faites des logiciels soumis à licence. La vérification que les licences détenues suffisent à répondre à cet usage doit alors être effectuée. En cas d'insuffisance, il devra être procédé à la désinstallation des exemplaires surnuméraires des logiciels concernés, ou de l'acquisition rapide des licences supplémentaires nécessaires.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T4-1.5 Documenter le SI

Disposer d'une documentation exhaustive et à jour du SI, de son architecture et de sa configuration est essentielle aussi bien à son exploitation journalière qu'à l'identification d'anomalie et qu'à l'exécution pertinente des procédures de réaction en cas d'incident, et participe fortement à la sécurité du SI.

Exigences :

⇒ L'architecture du SI, ses composants, leur configuration et leurs relations doivent être documentés, ainsi que les procédures associées.
⇒ La documentation du SI doit être maintenue à jour de manière continue.
⇒ L'accès à la documentation du SI doit être contrôlé, afin de garantir qu'elle ne peut être modifiée indûment, et que les parties de la documentation qui le nécessitent ne puissent être consultées que par les personnes habilitées.

Déclinaison en règles :

Règles sur la documentation du SI :

Réf.	Règles	Catégories de moyens du SI concernées
4.1.5.1	La documentation du SI devrait être constituée : • des informations sur le SI gérées dans le cadre des thématiques T4-1.1, T4-1.2 et T4-1.3 ; • de l'identification des services et des informations sensibles traitées par le SI ; • des schémas d'architecture du SI et de ses réseaux ; • des documentations des équipements, logiciels et services tiers utilisés destinées aux administrateurs du SI d'une part et aux utilisateurs d'autre part ; • du paramétrage de ces composants ; • pour chacun de ces composants ou ensembles cohérents de composants, des procédures d'installation, d'exploitation courante, d'utilisation courante par les utilisateurs (y compris l'administration « métier » du composant), de sauvegarde, de mise à jour, de détection d'anomalie, de réaction aux incidents, de retrait de service ; • des procédures générales de gestion du SI et de sa sécurité : gestion du plan d'adressage, du cloisonnement et du filtrage réseau, de gestion des prises réseau, d'attribution des postes téléphoniques, d'analyse des traces techniques… • des procédures spécifiques en cas de déclenchement du Plan de Continuité Informatique. La conservation du paramétrage d'un composant peut consister en l'écriture d'un document spécifique, mais peut aussi se suffire de la copie des fichiers de configuration qui définissent la configuration validée, ou	*Equipements d'infrastructure système et réseau, Equipements utilisateurs, Locaux*

	des copies d'écran montant l'intégralité des interfaces de paramétrage avec leurs valeurs validées.	
4.1.5.2	La documentation, selon la sensibilité des composants et des types d'informations concernés, ne doit pouvoir être : • accédée et consultée d'une part ; • modifiée d'autre part ; que selon les règles fixées par Commission habilitationet par les seules personnes en charge de SI et de sa sécurité, autorisées par l'autorité d'homologation.	*Documentation*
4.1.5.3	La documentation du SI devrait être maintenue à jour au fur et à mesure des modifications du SI ou de la configuration de ses composants.	*Documentation*
4.1.5.4	La documentation doit être protégée, préservée et être accessible aux personnes autorisées, même en cas d'incident susceptible de déclencher le Plan de Continuité Informatique (cf. T7-5).	*Documentation*
4.1.5.5	L'historique des informations d'inventaire et de la documentation du SI doit être conservé au moins pendant 1 an, et être protégé de la même manière que la documentation en cours.	*Documentation*

T4-2 Gérer le réseau local

T4-2.1 **Identifier ou authentifier chaque équipement** connecté au SI

Etant donné que le SI traite des données de santé à caractère personnel et bien que des mesures de cloisonnement de ces données puissent être mises en place, seuls les équipements autorisés doivent pouvoir y être connectés.

Exigence :

⇒ Tout équipement connecté au SI doit être identifié et, dans la mesure du possible ou si le contexte l'exige, être authentifié avant de pouvoir communiquer avec le reste du SI.

Déclinaison en règles :

Règles sur l'identification et l'authentification des équipements connectés au SI :

Réf.	Règles	Catégories de moyens du SI concernées
4.2.1.1	Tout équipement connecté au SI devrait préalablement avoir été répertorié dans l'inventaire et avoir été explicitement autorisé à être connecté au SI.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.2.1.2	L'infrastructure réseau du SI doit vérifier que tout équipement que l'on raccorde est effectivement autorisé à être connecté au SI. Au minimum, une autorisation d'accès au réseau basée sur le contrôle des adresses MAC doit être effectuée par l'infrastructure réseau. Si possible et afin de simplifier la gestion du réseau, l'autorisation d'accès au réseau doit se baser sur l'identification et l'authentification des équipements à l'aide du protocole 802.1x pour tous les équipements qui le supportent. Les équipements qui ne supportent pas 802.1x peuvent être identifiés par leur seule adresse MAC («MAC Authentication Bypass » par exemple), mais doivent alors être traités spécifiquement en étant affectés à un réseau virtuel distinct (voir règles T4-2.2).	*Equipements d'infrastructure/Réseaux*
4.2.1.3	Si un équipement est raccordé au réseau mais qu'il n'est pas autorisé (ou ni même connu), l'une des deux options suivantes doit être appliquée : • Soit l'équipement est automatiquement raccordé à un réseau « invité » considéré comme non sûr, qui peut offrir un ensemble de services restreints ; • Soit toute communication réseau entre l'équipement et le reste de l'infrastructure est interdite.	*Equipements d'infrastructure/Réseaux*
4.2.1.4	Les mesures d'authentification des équipements, de contrôle d'accès au réseau et de cloisonnement du réseau devraient permettre de parer aux risques d'usurpation d'adresse MAC et d'adresse réseau et, quand l'authentification n'est pas possible de manière fiable, de limiter au maximum l'impact d'une telle	*Equipements d'infrastructure/Réseaux*

	usurpation en restreignant les flux autorisés et en surveillant l'activité réseau.	
4.2.1.5	Pour ce qui concerne les terminaux mobiles susceptibles d'être directement raccordés à des environnements externes (ordinateur portable, ordiphone, …), l'autorisation d'accès au réseau interne devrait également être conditionnée par la vérification de conformité de l'équipement aux règles de la thématique T4-5 (notamment bon fonctionnement d'un antivirus à jour) dans une phase intermédiaire entre l'authentification et l'autorisation d'accès.	*Equipements d'infrastructure/Réseaux*
4.2.1.6	Une trace devrait être conservée de toute tentative de raccordement d'équipement, qu'elle soit autorisée ou non et de la suite qui lui est donnée. En cas de tentative de raccordement non autorisé et s'il n'est pas prévu d'accès « invité » dans cette situation, une alerte de sécurité doit être émise.	*Equipements d'infrastructure/Réseaux*
4.2.1.7	Il devrait être défini une procédure qui permette, à partir des informations qui caractérisent un flux observé en un point du réseau informatique, d'identifier et de localiser les équipements d'extrémité concernés. Une telle procédure s'appuie typiquement sur les adresses IP et MAC impliquées dans le flux, sur l'inventaire informatique, la documentation de l'architecture réseau, les informations fournies par les équipements réseau et sécurité. Le cas échéant ces informations sont centralisées à l'aide d'une plateforme d'administration du réseau.	*Equipements d'infrastructure/Réseaux*
4.2.1.8	Quand elles sont disponibles, les fonctions de détection et d'alerte en cas de changement d'équipement sur une prise (changement d'adresse MAC sur un port d'équipement réseau), voire de verrouillage de chaque port réseau sur l'adresse MAC légitimement associée, devraient être activées (dans la mesure où l'équipement connecté est supposé changer rarement).	*Equipements d'infrastructure/Réseaux*
4.2.1.9	Si un service de noms de domaines DNS est déployé en interne, la mise en œuvre de l'extension DNSSEC[10] est recommandée afin de garantir l'authenticité des informations transmises par ce service.	*Equipements d'infrastructure/Réseaux*

T4-2.2 Cloisonner les réseaux selon les besoins de sécurité

Les exigences liées aux usages du SI et aux caractéristiques des flux échangés sur son réseau peuvent être très variables au sein d'une même structure, selon l'utilisateur, l'équipement utilisé et le lieu d'utilisation.
Ainsi, l'accès à des données sensibles telles que le dossier médical d'un usager peut justifier le souhait que ces consultations soient effectuées depuis des postes de travail qui communiquent en « groupes fermés » avec le serveur de données. Ce même type d'accès, quand il est réalisé depuis des salles de soins peut, par exemple, exiger également une haute

[10] DNSSEC : « Domain Name System Security Extensions »

disponibilité du SI, justifiant une infrastructure du SI de fiabilité renforcée pour cet usage. Ailleurs, il faudra s'assurer que les flux de données générés par un appareil d'imagerie médicale ne perturbent pas, en saturant le réseau, le fonctionnement d'autres applications.
La prise en compte de ces différents besoins de sécurité induit une conception particulière de l'architecture réseau, au niveau de son infrastructure physique (le câblage et les équipements réseau) comme au niveau de son architecture logique (qui détermine comment les données circulent sur l'infrastructure physique).

Exigences :

⇒ Une cartographie des flux réseaux et des contraintes et besoins de sécurité associés doit être établie et maintenue à jour.
⇒ L'architecture du réseau doit être conçue, aux niveaux physique et logique, pour satisfaire ces besoins et contraintes, tout en tenant compte de la configuration des locaux de la structure et des contraintes d'exploitation du SI.
⇒ Des mesures de cloisonnement logique, voire physique, des flux doivent être mises en œuvre chaque fois que les besoins de sécurité ou de performance l'exigent.
⇒ Des mesures de redondance logique et physique de l'infrastructure réseau doivent être mises en œuvre chaque fois que les besoins de sécurité ou de performance l'exigent.

Déclinaison en règles :

Règles sur le cloisonnement du réseau :

Réf.	Règles	Catégories de moyens du SI concernées
4.2.2.1	Une cartographie des échanges réseaux entre les différents équipements connectés devrait être établie. Elle doit permettre de déterminer, au sein des différents équipements, « qui est censé communiquer avec qui ». Un second niveau de cartographie, plus détaillé, est prévu dans un deuxième temps par la règle 4.2.2.2.	*Catégorie de personnel (ex. responsable réseau)*
4.2.2.2	Un recensement des flux réseaux devrait être effectué et maintenu à jour. Il doit préciser, pour chaque flux : • le responsable technique du flux ; • le responsable métier du flux ; • le niveau d'exigence en termes de disponibilité et de confidentialité, ainsi que les autres contraintes (délai de transit, stabilité du délai de transit…) ; • les spécificités éventuelles (plage d'activité, forte volumétrie en continu ou par pics…).	*Catégorie de personnel (ex. responsable réseau)*
4.2.2.3	Les flux identifiés devraient être positionnés en fonction de leurs caractéristiques dans une ou plusieurs des catégories suivantes (indiquées pour exemple) : • Flux volumineux (ex. imagerie médicale, dont les flux doivent transiter dans des délais acceptables et sans perturber le reste des applications) ; • Flux à caractère vital (ex. consultation de dossier médical en zone de soins) ; • Flux confidentiel (ex. informations à caractère personnel) ;	*Catégorie de personnel (ex. responsable réseau)*

	• Flux Temps Réel (ex. téléphonie IP, visioconférence) ; • Flux d'origine non maîtrisée (ex. réseau « invités », wifi, Internet, …) ; • Flux d'administration et de supervision du SI et de la sécurité ; • Flux standard (par défaut). Ces catégories constituent une base essentielle pour la définition de l'architecture et le paramétrage du réseau et de son cloisonnement.	
4.2.2.4	Le cloisonnement du réseau peut s'appuyer sur deux techniques, si nécessaire cumulables, qui seront choisies selon leur adéquation au besoin et leur disponibilité sur les équipements réseau utilisés : • La mise en œuvre de réseaux virtuels (« VLAN ») qui offrent un cloisonnement « logique » des réseaux tout en partageant une même infrastructure physique et permettent une grande souplesse de gestion ; • La mise en œuvre de segments réseau physique et d'équipements séparés et dédiés. Si la structure partage des locaux avec d'autres entités juridiques, son réseau doit être strictement cloisonné vis-à-vis de ceux de ces entités. Ce cloisonnement devrait s'appuyer de préférence sur une séparation physique complète, ou à défaut par un cloisonnement logique dont les modalités doivent être validés par le Responsable de la SSI et par le responsable du SI.	*Equipements d'infrastructure/Réseaux*
4.2.2.5	Les flux confidentiels et les flux sensibles (flux d'administration et de supervision des systèmes et des équipements réseaux) devraient être confinés, par la mise en œuvre de cloisonnement, aux seuls équipements dont ils sont issus ou auxquels ils sont destinés (hors infrastructure réseau). A défaut d'un tel cloisonnement, ces flux doivent utiliser des canaux de communication qui mettent en œuvre un chiffrement et un contrôle d'intégrité des données (SSH, HTTPS, SSL, TLS…) dont les caractéristiques et paramètres doivent être conformes aux règles de l'art (notamment, bien identifier les versions et options de protocoles à ne pas utiliser pour raison de failles de sécurités). La règle 6.5.1.9 doit alors être respectée pour le choix des dispositifs utilisés.	*Equipements d'infrastructure/Réseaux*
4.2.2.6	Les flux d'origine non maîtrisée (ex. un réseau « invités » pour la connexion des ordinateurs portable des visiteurs) doivent être confinés dans un réseau dédié.	*Equipements d'infrastructure/Réseaux*
4.2.2.7	Les accès effectués à distance par des utilisateurs internes et autorisés de la structure depuis des postes nomades (« accès nomades ») devraient être confinés dans un réseau dédié.	*Equipements d'infrastructure/Réseaux*
4.2.2.8	Les accès nomades doivent :	*Equipements d'infrastructure/Réseaux*

	• n'être possibles que depuis les terminaux mobiles fournis à l'utilisateur par la structure et conformes aux règles de T4-5 ; • être réalisés via un canal de communication sécurisé de type VPN dont la sécurité est maîtrisée soit par la structure elle-même, soit par un prestataire de confiance ; • s'appuyer sur des mécanismes d'authentification conformes au Référentiel d'authentification des acteurs de santé [Réf. n°6.12] et mis en œuvre selon les modalités présentées dans l'annexe B3 du RGS [Réf. n°9].	
4.2.2.9	Les besoins liés aux performances du réseau, par exemple pour les flux volumineux ou les flux Temps Réel, peuvent être traités : • soit par paramétrage de la qualité de service qui leur est appliquée (ou qui est appliquée au réseau virtuel auquel sont affectés les équipements concernés) ; • soit par la mise en œuvre d'un réseau physique dédié.	*Equipements d'infrastructure/Réseaux*
4.2.2.10	Les besoins de haute disponibilité du réseau, par exemple pour les flux à caractère vital, sont traités par la mise en œuvre de liaisons physiques et équipements réseau qui permettent des chemins multiples entre l'origine et la destination des flux et l'activation de protocoles réseau qui permettent une reconfiguration automatiques des chemins empruntés par les flux en cas de défaillance d'une partie du réseau.	*Equipements d'infrastructure/Réseaux*
4.2.2.11	L'interconnexion de « bulles réseau », cloisonnées pour des raisons autres que les seules performances ou disponibilité, doit être réalisée exclusivement via des équipements de sécurité adaptés (pare-feu, passerelle…), selon le principe de « liste blanche » : tout flux qui n'est pas explicitement autorisé est interdit.	*Equipements d'infrastructure/Réseaux*
4.2.2.12	Outre les exigences de cloisonnement évoquées par ailleurs, les environnements suivants devraient également, sauf impossibilité technique, être cloisonnés : • serveurs de production ; • systèmes de stockage de données (baies de disques en réseau...) et dispositifs de sauvegarde ; • postes et équipements pour les activités normales des utilisateurs ; • environnement de développement ; • environnement de recette ; • environnement de formation ; • environnement d'administration des systèmes, des réseaux et de la SSI ; • prises réseau et équipements situés dans les lieux librement accessibles au public ;	*Equipements d'infrastructure/Réseaux*

	• équipements qui ont des failles de sécurité connues sans correctif disponible à court terme et dont l'utilisation reste indispensable.	
4.2.2.13	Les prises réseau situées dans les lieux librement accessibles au public et qui ne sont pas utilisées devraient être désactivées au niveau des équipements réseau ou physiquement déconnectées au niveau des baies de brassage réseau.	*Equipements d'infrastructure/Réseaux*

T4-3 Gérer la connexion Internet

T4-3.1 Sécuriser la connexion Internet

Toute connexion du SI à un autre SI ou à un réseau tiers et *a fortiori* à Internet, l'expose à des risques supplémentaires auxquels il convient de parer. Des précautions spécifiques doivent être prises pour sécuriser cette connexion.

Exigences :

⇒ Seuls les flux prévus et autorisés doivent pouvoir transiter entre le SI de la structure et les réseaux externes, dont Internet en particulier. Ce contrôle doit être assuré par un dispositif de filtrage de flux réseau.

⇒ Si possible, un contrôle des flux au niveau applicatif doit être effectué sur les flux en provenance ou à destination d'Internet.

⇒ Tout dispositif directement accessible depuis Internet, par exemple en vue de fournir un service (serveur web, …), étant destinataire de flux d'origine non maîtrisée, doit être positionné dans une zone réseau tampon cloisonnée, dite « zone démilitarisée » ou « DMZ », isolée du reste du SI par un dispositif de sécurité adéquat.

⇒ Les flux en provenance ou à destination d'Internet doivent faire l'objet d'une détection et d'un blocage automatique des contenus malveillants.

⇒ Si la connexion Internet est nécessaire à l'exécution de processus critiques, des mesures garantissant le niveau de disponibilité requis doivent être mises en œuvre.

Déclinaison en règles :

Règles sur la sécurisation de la connexion Internet :

Réf.	Règles	Catégories de moyens du SI concernées
4.3.1.1	La connexion à Internet doit être séparée du reste du SI par au moins un dispositif de filtrage réseau (« pare-feu » ou « firewall »).	*Equipements d'infrastructure/Réseaux*
4.3.1.2	Les dispositifs de filtrage réseau devraient être paramétrés sur un principe de « liste blanche » : tout flux qui n'est pas explicitement autorisé est interdit.	*Equipements d'infrastructure/Réseaux*
4.3.1.3	Les flux réseau « sortants », issus du SI à destination d'Internet, doivent transiter par des dispositifs relais ou « proxy », qui assurent une vérification des échanges du point de vue protocolaire et qui intègrent une détection et un blocage automatique des contenus potentiellement malveillants. Cette règle doit notamment être appliquée aux flux de type : • Web (HTTP), par un relai « proxy web » • Transferts de fichiers (FTP) • Messagerie (SMTP) • Noms de domaines (DNS) On appelle ici « flux sortants » les données échangées dans les deux sens avec Internet mais résultant de l'action d'un utilisateur interne ou d'un dispositif interne (ex : consultation web Internet, envoi de courrier électronique).	*Equipements d'infrastructure/Réseaux*
4.3.1.4	Les dispositifs relais pour les flux « sortants » doivent être hébergés dans une DMZ dédiée et ne doivent pouvoir communiquer avec Internet d'une part et avec	*Equipements d'infrastructure/Réseaux (ex.Pare-feu, Proxy web)*

	le reste du SI d'autre part, qu'à travers un dispositif de filtrage.	
4.3.1.5	Les services offerts par le SI et destinés à être consultés depuis Internet doivent être hébergés sur des équipements dédiés. Ces équipements doivent être exclusivement rattachés à une DMZ dédiée à ces accès « entrants » qui ne peut communiquer avec Internet d'une part et avec le reste du SI d'autre part qu'à travers un dispositif de filtrage. Exemples de services concernés : • Service DNS public (serveurs primaire et secondaires) ; • Service web public ; • Service web « extranet » ; • Service de messagerie entrant (SMTP) ; • Service de consultation de messagerie depuis Internet (IMAP, POP3… à mettre en œuvre uniquement avec la version « sécurisée » de ces protocoles) Si l'architecture réseau ne permet pas de mettre en place une telle DMZ, l'hébergement externe (chez un prestataire) de ces services doit être envisagé. Dans certains cas, les enjeux de sécurité de l'information liés à certains services (ex. intranets, certains extranets) peuvent justifier qu'ils soient positionnés dans une DMZ différente de celle qui héberge les services accessibles à tout public (ex. web institutionnel « vitrine »)	*Equipements d'infrastructure/Réseaux (ex. Pare-feu)*
4.3.1.6	Les flux réseau « entrants », issus d'Internet à destination de services accessibles depuis Internet, doivent transiter par des dispositifs relais ou « reverse proxy », qui assurent une vérification des échanges du point de vue protocolaire et qui intègrent une détection et un blocage automatique des contenus potentiellement malveillants, chaque fois que ce type de dispositif de sécurité est disponible. Cette règle doit notamment être appliquée aux flux de type : • Web (HTTP, HTTPS), via un « reverse proxy » • Transferts de fichiers (FTP) • Messagerie (SMTP) L'utilisation d'un « reverse proxy », qui peut être mutualisé entre plusieurs services ouverts sur Internet, est particulièrement importante pour détecter et bloquer des vulnérabilités « génériques » potentiellement présentes dans les applications web. Elle permet aussi, en cas de vulnérabilité identifiée, de mettre rapidement en place des mesures de protection, dans l'attente de l'installation d'un correctif spécifique à l'application.	*Equipements d'infrastructure/Réseaux*
4.3.1.7	Quand le SI s'appuie sur une architecture virtualisée, les machines virtuelles utilisées pour les DMZ en communication directe avec Internet devraient être	*Equipements d'infrastructure/Serveurs virtualisés*

	positionnées sur un ou des serveurs physiques dédiés et distincts des serveurs physiques utilisés pour le SI interne.	
4.3.1.8	Si la structure n'est pas en mesure de mettre en œuvre les dispositifs requis par les règles 4.3.1.1 à 4.3.1.7, ou si les postes nécessitant un accès à Internet doivent, pour les besoins de l'application envisagée, être configurés selon des modalités qui dégradent leur sécurisation et mettent de fait à risque le reste du SI : • les postes accédant à Internet doivent être dédiés à cet usage et physiquement séparés du reste du réseau ; • l'accès à Internet doit desservir ces postes uniquement ; • la sécurisation et le maintien à jour des configurations de ces postes doit être réalisées spécifiquement, ces postes n'ayant pas accès au réseau « interne » de la structure ; • ces postes doivent faire l'objet d'une surveillance régulière.	Equipements utilisateurs/Terminaux
4.3.1.9	Si les équipements de raccordement (routeurs) à des réseaux tiers (Internet ou autres) mettent en œuvre un protocole de routage dynamique de type « IGP » (ex. RIP, IGRP, E-IGRP, OSPF), ce protocole doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. De plus, la configuration du protocole de routage dynamique doit activer les fonctions de sécurisation du protocole (authentification des messages notamment) recommandées par l'état de l'art (ex. mise en œuvre du MESSAGE-DIGEST-KEY).	*Equipements d'infrastructure/Réseaux (ex. Routeurs d'accès)*

T4-3.2 Limiter les accès Internet en conformité avec la Charte d'Utilisation des Ressources Informatiques

L'accès à Internet depuis le SI de la structure présente plusieurs risques du point de vue de la sécurité du SI, comme par exemple :

- La divulgation publique, volontaire ou par inadvertance, d'informations professionnelles sensibles ;
- L'accès à des sites web illégaux ou la violation des droits liés à la propriété intellectuelle (téléchargement illégaux de musique, films, logiciels…) qui engagent la responsabilité de la structure ;
- L'introduction de logiciels malveillants dans le SI par navigation sur des sites web piratés à l'insu de leurs propriétaires ;
- La tenue de propos illégaux (racisme, appel à la violence…) ou gênants par un utilisateur sous son identité professionnelle (son adresse de messagerie par exemple), portant ainsi atteinte à l'image de la structure.

La Charte d'Utilisation des Ressources Informatiques qui doit être mise en place dans la structure doit normalement traiter ces questions du point de vue du comportement auquel s'engagent les utilisateurs.

Il convient cependant de mettre en œuvre les mesures :

- Qui permettent de bloquer les comportements à risques que pourrait avoir un utilisateur par mégarde ou par curiosité ;
- Qui sont nécessaires à la détection et à la réaction dans le cas où un utilisateur ne respecterait pas les engagements qu'il a pris.

Exigences :

⇒ L'accès à Internet depuis le SI ne doit être possible qu'aux utilisateurs ou services autorisés et préalablement authentifiés.

⇒ L'accès aux sites web qui sont exclus par la Charte d'Utilisation des Ressources Informatique du fait de leur nature doit être bloqué (sauf dérogation prévue par la charte).

⇒ L'accès aux sites web qui sont connus pour présenter des risques pour la sécurité du SI doit être bloqué.

⇒ L'accès à des sites web en mode sécurisé (HTTPS, TLS, SSL) ne doit être possible que pour une liste « blanche » de sites de confiance autorisés. En effet, ce type de connexion interdit toute détection de contenu dangereux ou non conforme aux exigences de sécurité et de manière générale permet de contourner tout contrôle sur les sites accédés comme sur la nature des communications.

⇒ L'accès à des services autres que web doit être autorisé au cas par cas, après analyse détaillée des risques induits et ce quel que soit le protocole réseau utilisé (TCP/IP, UDP/IP ou autre).

Déclinaison en règles :

Règles sur le contrôle des accès à Internet :

Réf.	Règles	Catégories de moyens du SI concernées
4.3.2.1	Le dispositif relai « proxy web » qui permet l'accès à Internet aux utilisateurs internes du SI pour la navigation web, voire pour le transfert de fichiers, doit assurer l'authentification de tout utilisateur avant de lui permettre cet accès s'il y est autorisé.	*Equipements d'infrastructure/Réseaux (ex. Proxy web)*
4.3.2.2	Le dispositif relai « proxy web » doit intégrer une catégorisation des sites web d'Internet et être paramétré pour n'autoriser l'accès qu'aux sites appartenant à des catégories légitimes au regard de la Charte d'Utilisation des Ressources Informatiques et non risquées du point de vue SSI. La catégorisation des sites web doit être publiée régulièrement par le fournisseur (ou l'éditeur) du dispositif relai et mise à jour automatiquement. Une attribution de droits d'accès différenciés aux catégories de sites web doit être possible pour certains utilisateurs. C'est le cas, par exemple, pour les exploitants informatiques ou pour les personnes en charge de la sécurité du SI, qui doivent pouvoir accéder à certains sites d'information sur la SSI souvent catégorisés comme « risqués » dans les dispositifs de filtrage web du fait des sujets traités (protections mais aussi méthodes de piratage informatiques…).	*Equipements d'infrastructure/Réseaux*
4.3.2.3	Le dispositif relai « proxy web » devrait bloquer toute communication web en mode « sécurisé » (SSL/TLS) vers les sites ne faisant pas partie d'une liste blanche	*Equipements d'infrastructure/Réseaux*

	de sites web auxquels l'accès est nécessaire à l'activité de la structure. Un site web ne doit être ajouté à cette liste blanche qu'après vérification que la demande d'accès est justifiée et validée par un responsable métier et que le site lui-même ne présente pas de risque pour la sécurité (pas de possibilité de rebond vers un autre site ou d'accès à des contenus interdits par la Charte, pas de mise en œuvre de logiciels qui s'installent dans le navigateur de l'utilisateur, …). Une recherche sur Internet ou sur le site de l'éditeur du « proxy web » peut donner ce type de renseignements. Il est souhaitable qu'une attribution de droits d'accès différenciés aux sites web en mode sécurisé soit possible afin de pouvoir gérer de manière souple les inévitables besoins de dérogation sans devoir étendre cette possibilité d'accès à l'ensemble des utilisateurs.	
4.3.2.4	Une procédure de demande d'ouverture de flux vers Internet pour d'autres protocoles que web et de décision d'autorisation ou de refus, doit être définie.	*Catégorie de personnel (ex. Responsable de la SSI, Responsable réseau)*
4.3.2.5	Cette procédure doit imposer, pour chaque autorisation d'ouverture de flux, de restreindre autant que possible, outre le protocole utilisé, aussi bien la destination (externe) de la connexion autorisée que son origine (interne) et le cas échant de la limiter à certaines plages horaires (si le dispositif de filtrage supporte cette fonctionnalité). Si le dispositif de filtrage permet une authentification préalable de l'utilisateur pour ce protocole, cette fonctionnalité doit être mise en œuvre.	*Catégorie de personnel (ex. Responsable de la SSI, Responsable réseau)*
4.3.2.6	Les autorisations d'ouverture de flux devraient être données pour une durée limitée et doivent faire l'objet d'une revalidation régulière du besoin auprès du responsable métier concerné, selon une périodicité au moins annuelle.	*Catégorie de personnel (ex. Responsable de la SSI, Responsable réseau)*

T4-3.3 Conserver une trace des connexions Internet

La connexion Internet constitue un point majeur d'exposition aux risques de sécurité pour le SI. La génération et la conservation de traces des accès à Internet permettent la détection d'activités anormales et l'investigation suite à un incident de sécurité.

Exigences :

⇒ Toute connexion ou tentative de connexion à un service web doit donner lieu à la génération d'une trace , de niveau application comme de niveau réseau, de cet accès.

⇒ Toute connexion ou tentative de connexion autre qu'à un service web doit donner lieu au minimum à une trace de niveau réseau.

⇒ Les autres types d'échanges réseau, autorisés ou bloqués (en mode non connecté par exemple, tels que DNS, ICMP…) doivent donner lieu à un suivi, au minimum par compteurs d'activité.

⇒ Pour pouvoir être utilisées si nécessaire dans le cadre d'une enquête, l'intégrité des traces doit être assurée. Par ailleurs, les traces constituent des données à caractère personnel puisque les utilisateurs concernés sont identifiés. Elles doivent être gérées comme telles, notamment du point de vue de :

- Leur protection contre les consultations non autorisées ;
- Leur protection contre toute modification ;
- Leur suppression après un délai de rétention « proportionné » au vu des objectifs poursuivis.

Déclinaison en règles :

Règles sur la conservation des traces des connexions Internet :

Réf.	Règles	Catégories de moyens du SI concernées
4.3.3.1	Les dispositifs relais « proxy web » doivent être paramétrés pour générer une trace de toute connexion qu'ils traitent. Cette trace doit comporter au minimum les informations suivantes : • Date et heure de l'évènement • Identification de l'utilisateur • Etat d'authentification de l'utilisateur • Equipement à l'origine de la requête : adresse IP, port TCP • Requête HTTP : commande, url demandée, volume transmis • Etat d'autorisation de la requête par le proxy • Raison du refus éventuel de la requête (ex : catégorie de site interdite) • Destination de la connexion : adresse IP et port TCP • Statut de la réponse à la requête • Volume transféré dans chaque sens • Durée de la connexion • Raison du blocage éventuel de la réponse par le proxy (ex : nature du contenu malveillant détecté, site web n'appartenant pas à une catégorie de sites autorisée…)	*Equipements d'infrastructure/Réseaux*
4.3.3.2	Les équipements de filtrage réseau doivent être paramétrés pour générer une trace pour tout flux autorisé vers ou depuis Internet. Cette trace doit comporter au minimum les informations suivantes : • Date et heure de l'évènement • Equipement à l'origine du flux : adresse IP • Equipement destinataire du flux : adresse IP • Protocole réseau : TCP, UDP, ICMP, … • Port ou service source, Port ou service destination • Etat d'autorisation par l'équipement de filtrage (autorisé ou bloqué) • Volume transféré dans chaque sens • Durée de la connexion (quand applicable)	*Equipements d'infrastructure/Réseaux*
4.3.3.3	Les équipements de filtrage réseau doivent être paramétrés pour générer une trace, sur le même	*Equipements d'infrastructure/Réseaux*

	modèle, pour tout flux, autorisé ou bloqué, issu d'une DMZ.	
4.3.3.4	Il est recommandé que les équipements de filtrage réseau génèrent également une trace, sur le même modèle, pour tout flux bloqué issus du SI interne et à destination d'Internet ou des DMZ.	*Equipements d'infrastructure/Réseaux*
4.3.3.5	Les traces générées doivent être gérées conformément aux règles de la thématique 7-2.2.	*Equipements d'infrastructure/Réseaux*
4.3.3.6	Les utilisateurs du SI doivent être informés que les accès à Internet sont tracés à des fins de sécurité.	*Catégorie de personnel (ex. Responsable de la SSI)*

T4-4 Gérer les connexions sans fil

Les règles de sécurité proposées pour cette thématique sont issues du « Guide pratique spécifique pour la mise en place d'un accès Wifi » [Réf. n°6.8] du corpus documentaire PGSSI-S.

T4-4.1 Sécuriser la mise en place d'un point d'accès Wifi

La mise en place d'un réseau sans fil (Wifi, Bluetooth, ZigBee…) est une opération qui doit être traitée avec attention. En effet, contrairement à un réseau filaire, un réseau sans fil est, d'un point de vue technique, potentiellement accessible à toute personne qui se trouve dans sa zone de couverture radio. Cette zone s'étend souvent au-delà des limites du site de la structure et dans des lieux accessibles au public.
Il est donc essentiel de mettre en œuvre les mesures qui garantissent que, bien que cet accès technique aux ondes radio du réseau sans fil soit possible pour toute personne, seules les personnes autorisées aient accès aux ressources prévues du SI de la structure.
Il est important de souligner que tout système de communication usuel qui s'appuie sur des ondes radio peut facilement être rendu temporairement indisponible par une personne malveillante. Ce point doit impérativement être pris en compte avant tout déploiement de dispositif critique qui nécessiterait ce type de communication.

Exigences :

⇒ Les équipements point d'accès Wifi doivent supporter les standards et protocoles de communication considérés comme fiables du point de vus SSI.

⇒ Les protocoles de sécurité qui doivent être utilisés sont, parmi ceux supportés par les équipements points d'accès Wifi, ceux qui apportent les meilleures garanties de sécurité. Ils doivent être mis en œuvre en conformité avec les règles de l'art.

⇒ Le positionnement, la puissance d'émission et le paramétrage des équipements point d'accès Wifi doivent être définis de telle sorte que ces équipements ne créent d'interférence ni entre eux, ni avec d'autres équipements et qu'ils limitent autant que possible la portée efficace du réseau Wifi à ses zones d'utilisation prévues.

Déclinaison en règles :

Règles sur la sécurisation des points d'accès Wifi :

Réf.	Règles	Catégories de moyens du SI concernées
4.4.1.1	Seul le personnel ou les sociétés désignées par le responsable du SI, ou leurs délégataires en charge	*Equipements d'infrastructure/Réseaux*

	de la gestion des réseaux informatiques, peuvent mettre en place et gérer un point d'accès Wifi. Une procédure d'installation et de sécurisation des points d'accès devrait être formalisée. Elle doit être mise en œuvre lors de chaque installation d'un nouvel équipement.	
4.4.1.2	Le point d'accès Wifi doit être compatible avec la norme IEEE 802.11. Le choix des canaux de transmission du Wifi doit être effectué de manière à ne pas créer d'interférences avec d'autres équipements ou entre les différents réseaux wifi mis en œuvre (accès PS, accès technique et accès invité).	*Equipements d'infrastructure/Réseaux*
4.4.1.3	Pour prévenir toute interférence potentielle, les recommandations des fournisseurs d'équipements de santé installés à portée du point d'accès Wifi devraient être respectées. Une étude doit être menée dans ce sens avant toute mise en œuvre de point d'accès Wifi.	*Equipements d'infrastructure/Réseaux*
4.4.1.4	Le nombre de bornes, leur positionnement ainsi que la puissance du signal Wifi doivent être adaptés à la superficie de la zone à couvrir.	*Equipements d'infrastructure/Réseaux*
4.4.1.5	Il convient de prévoir, pour les équipements connectés par Wifi, un mode dégradé permettant de garantir la continuité des activités en cas de dysfonctionnement des communications Wifi.	*Equipements d'infrastructure/Réseaux*
4.4.1.6	Comme tous les équipements connectés au réseau, les équipements Wifi (bornes, câbles d'accès…) doivent, autant que faire se peut, être protégés et non accessibles au public afin d'éviter : • un accès direct au réseau interne du SI, par exemple en déconnectant le câble de connexion et en l'utilisant directement sur son matériel ; • ou une réinitialisation non contrôlée de l'équipement. Cette protection peut être mise en œuvre par une combinaison de dispositions physiques et de configuration du matériel par exemple routeur wifi dans une boite fermée à clef, routeur wifi positionné dans le champ de vision du personnel, désactivation des connecteurs RJ45 femelles non utilisés, authentification du routeur sur le réseau filaire…	*Equipements d'infrastructure/Réseaux*
4.4.1.7	L'identifiant du réseau Wifi (SSID) devrait être anonymisé afin d'éviter de faire apparaitre le nom de l'opérateur internet et de donner toute information qui permettrait à une personne mal intentionnée de se connecter au réseau. Il peut également être rendu invisible, nécessitant ainsi, lors de sa première connexion, que l'utilisateur entre manuellement les informations du SSID au lieu de la sélectionner dans la liste des réseaux. Il est cependant à noter que cette mesure n'est pas suffisante pour sécuriser l'accès au wifi bien qu'elle	*Equipements d'infrastructure/Réseaux*

	permette de réduire le nombre de tentatives de connexions frauduleuses.	
4.4.1.8	Un contrôle d'accès des équipements connectés au réseau interne du SI via le Wifi doit être effectué. Il doit être réalisé en priorité par l'utilisation du protocole 802.1X[11]. Les réseaux Wifi et internes du SI doivent être séparés au moyen d'un dispositif de filtrage (firewall) n'autorisant que les services, les protocoles et les ports de communication nécessaires aux flux métiers prévus.	*Equipements d'infrastructure/Réseaux*
4.4.1.9	Les équipements utilisés pour se connecter (terminaux professionnels et équipements de santé) doivent être configurés, lors de leur installation, pour restreindre l'association automatique aux seuls réseaux Wifi légitimes et exigeant une authentification 802.1X dans le but d'éviter une connexion involontaire à un réseau malveillant qui se ferait passer pour un réseau légitime.	*Equipements d'infrastructure/Réseaux*
4.4.1.10	Le mot de passe par défaut du compte administrateur de la borne Wifi doit être modifié. Un mot de passe fort de 10 caractères au minimum (recours à la fois de caractères alphabétiques, numériques, spéciaux et non triviaux) doit être utilisé.	*Equipements d'infrastructure/Réseaux*
4.4.1.11	Seuls les services, les protocoles et les ports de communication nécessaires au fonctionnement et à l'utilisation de la borne Wifi doivent être activés. Par exemple, le protocole DNS-SD doit notamment être désactivé quand le parc d'équipement ne nécessite pas de reconfiguration fréquente.	*Equipements d'infrastructure/Réseaux*
4.4.1.12	L'authentification des utilisateurs et la confidentialité des données doivent être assurées par la mise en place de mécanismes s'appuyant sur la norme WPA2-entreprise (standard 802.1X et protocole EAP, idéalement EAP-TLS) avec utilisation de l'algorithme de chiffrement AES-CCMP. Le site de l'ANSSI décrit ces différents mécanismes : (http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-liaisons-sans-fil/recommandations-de-securite-relatives-aux-reseaux-wifi.html). A défaut, le protocole PEAP/EAP-MSCHAPv2 peut être utilisé en lieu et place du protocole EAP-TLS.	*Equipements d'infrastructure/Réseaux*
4.4.1.13	Le certificat serveur présenté par le point d'accès Wifi configuré en WPA2-Entreprise doit être signé par une autorité de certification de confiance pour les postes clients.	*Equipements d'infrastructure/Réseaux*
4.4.1.14	Lorsque des mécanismes d'authentification robustes (802.1X) ne peuvent être utilisés, l'authentification des utilisateurs et la confidentialité des données doivent être assurées par le mode WPA2-PSK (WPA2-Personnel) avec utilisation de l'algorithme de	*Equipements d'infrastructure/Réseaux*

[11] Protocole standard lié à la sécurité des réseaux informatiques, il permet de contrôler l'accès aux équipements d'infrastructures réseau.

	chiffrement AES-CCMP. La clé de sécurité pour WPA2 doit être conforme aux règles d'élaboration de mots de passe non triviaux et changée dès l'installation, puis régulièrement.	
4.4.1.15	Les fonctions de simplification de l'authentification de type WPS (Wifi Protected Setup) doivent être désactivées.	*Equipements d'infrastructure/Réseaux*
4.4.1.16	Un filtrage de l'accès aux sites web doit être mis en place conformément à la charte d'utilisation d'accès et d'usage du SI de la structure.	*Equipements d'infrastructure/Réseaux*

T4-4.2 Assurer l'exploitation d'un point d'accès Wifi

Exigences :

⇒ L'exploitation des points d'accès Wifi doit être réalisée en conformité avec les bonnes pratiques de sécurité.

Déclinaison en règles :

Règles sur l'exploitation d'un accès Wifi :

Réf.	Règles	Catégories de moyens du SI concernées
4.4.2.1	L'administration d'un point d'accès Wifi doit être réalisée depuis le réseau filaire interne du SI, de préférence à partir d'un réseau d'administration logiquement séparé et en utilisant un protocole sécurisé (ex : HTTPS, SSH, …). Les interfaces d'administration du point d'accès ne doivent pas être disponibles depuis le réseau Wifi.	*Equipements d'infrastructure/Réseaux*
4.4.2.2	Le micro-logiciel de chaque point d'accès Wifi doit être maintenu et mis à jour régulièrement.	*Equipements d'infrastructure/Réseaux*
4.4.2.3	Pour s'assurer de la compatibilité des matériels utilisés pour la mise en œuvre d'un point d'accès Wifi, des tests préalables doivent être réalisés.	*Equipements d'infrastructure/Réseaux*
4.4.2.4	La gestion des traces doit être activée sur les points d'accès Wifi. Les traces doivent être centralisées et analysées régulièrement pour identifier des anomalies potentielles dans les accès effectués (heures d'accès, volumes de données échangées…).	*Equipements d'infrastructure/Réseaux*
4.4.2.5	Les traces générées par les points d'accès Wifi doivent être gérées conformément aux règles de la thématique 7-2.2.	*Equipements d'infrastructure/Réseaux*
4.4.2.6	Le réseau du SI ne doit pas accueillir de bornes Wifi non gérées par le responsable du SI (ex. bornes Wifi « pirates »). Des contrôles devraient être menés régulièrement pour s'en assurer.	*Equipements d'infrastructure/Réseaux*

T4-4.3 Sécuriser la mise en place d'un point d'accès Wifi « invité »

Exigences :

⇒ L'accès d'un utilisateur au réseau Wifi invité ne doit être autorisé que sur une base individuelle et temporaire et doit mettre en œuvre un moyen d'authentification de l'utilisateur.

⇒ L'accès d'un utilisateur au réseau Wifi invité ne doit être autorisé qu'avec l'acceptation par l'utilisateur des conditions d'utilisation (conformes à la Charte d'Utilisation des Ressources Informatiques), de l'engagement de sa responsabilité sur l'usage qu'il fait de cet accès et de reconnaissance de la réception du moyen d'authentification qui lui est attribué.

⇒ Le réseau Wifi invité doit être strictement cloisonné. Tout accès à un service fourni par le SI doit être réalisé via un équipement de sécurité qui, si la sensibilité du service le justifie, authentifie l'utilisateur avant de l'autoriser.

⇒ L'accès à Internet depuis le réseau Wifi invité doit respecter les règles relatives à la sécurisation de l'accès Internet.

Déclinaison en règles :

Règles sur la mise en place d'un accès Wifi « invité » :

Réf.	Règles	Catégories de moyens du SI concernées
4.4.3.1	Les règles des thématiques précédentes (T4-4.1 et T4-4.2) sont également applicables aux points d'accès wifi « invité », à l'exception des règles 4.4.1.8, 4.4.1.9, 4.4.1.12, 4.4.1.13, 4.4.1.14 et 4.4.2.4 qui ne s'appliquent pas dans ce cas.	*Equipements d'infrastructure/Réseaux*
4.4.3.2	Le SI interne doit être strictement cloisonné du réseau Wifi mis à disposition des invités pour ne pas permettre l'accès aux ressources du SI interne. Dans l'idéal, l'accès invité doit disposer d'une infrastructure dédiée à cet usage et ne donnant accès à aucune ressource du SI interne. A défaut, un cloisonnement logique doit être mis en œuvre.	*Equipements d'infrastructure/Réseaux*
4.4.3.3	L'accès Wifi Invité doit être conditionné soit par un code d'accès disponible à l'intérieur des locaux et changé régulièrement soit par un code personnel attribué de manière individuelle suite à une procédure d'enregistrement (accueil par exemple) soit éventuellement après enregistrement auprès d'un serveur/portail 802.1X ou d'un portail captif.	*Equipements d'infrastructure/Réseaux*
4.4.3.4	Dans le cas où un code personnel est nécessaire pour l'accès Wifi invité, la procédure d'enregistrement doit comporter l'approbation par l'invité des conditions d'utilisation de l'accès Wifi Invité ou l'acceptation obligatoire de ces éléments lors de sa demande de connexion au réseau. Elle peut comporter la vérification et la consignation de l'identité du demandeur.	*Equipements d'infrastructure/Réseaux*
4.4.3.5	Une trace des connexions Wifi des utilisateurs doit comporter les éléments suivants s'ils sont disponibles : • les informations permettant d'identifier l'utilisateur ; • les données relatives aux équipements terminaux de communication utilisés (par	*Equipements d'infrastructure/Réseaux*

	exemple adresse MAC, type d'équipement, adresse IP attribuée…) ; • les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication (protocole utilisé http, https, …) ; • les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; les données permettant d'identifier le ou les destinataires de la communication (par exemple adresse IP ou nom DNS du site web consulté).	
4.4.3.6	La durée de connexion d'un invité doit être temporaire et sa durée explicitement indiquée lors de l'authentification au service. Dès lors que le délai est dépassé, la connexion wifi doit être automatiquement interrompue.	*Equipements d'infrastructure/Réseaux*
4.4.3.7	Des éléments de sensibilisation à la sécurité doivent être portés à la connaissance des « invités » utilisant le wifi notamment concernant le caractère public de l'accès mis à disposition, le fait qu'il n'est pas spécifiquement sécurisé par la structure hébergeant cet accès (ex. pas d'antivirus, pas de protection anti-intrusion des terminaux se connectant à l'accès wifi…) et les conditions d'usage (ex. engagement de sa responsabilité en cas de non-respect de la loi, existence éventuelle de mesures de filtrage et de trace des accès et des droits dont il dispose sur ce sujet…). Ces éléments peuvent par exemple être intégrés aux supports d'informations diffusés aux utilisateurs (ex. livret d'accueil, affiches en zone d'admission, dans les chambres et/ou dans les espaces usagers internet, page d'accueil du portail d'accès au wifi…).	*Equipements d'infrastructure/Réseaux*
4.4.3.8	Un filtrage doit être mis en place afin d'interdire l'accès aux sites web dont la consultation est interdite aux mineurs ou dont le contenu est illégal. Un filtrage plus contraignant peut être mis en place conformément à la charte d'utilisation d'accès et d'usage du SI de la structure.	*Equipements d'infrastructure/Réseaux*

T4-5 Protéger l'accès aux systèmes (postes de travail, serveurs, équipements réseau, dispositifs connectés, …)

Afin de permettre une gestion maîtrisée et efficace du SI, et ce d'autant plus que le nombre d'utilisateurs et d'équipements est important, il est recommandé que des outils de gestion centralisée du SI, et en particulier de sa sécurité, soient mis en œuvre, pour permettre aux administrateurs du SI de disposer aussi bien d'une vue et d'une capacité d'action globale que de possibilités d'automatisation de traitements quotidiens. Cette centralisation des outils concerne par exemple :

- *la gestion des utilisateurs et de leurs autorisations,*
- *la configuration et la supervision des équipements réseau,*
- *la supervisions des serveurs, baies de disques, autocommutateurs, onduleurs dédies au SI…,*
- *le paramétrage et le suivi des installations et mises à jour de logiciels,*
- *le paramétrage et la supervision des antivirus,*
- *la gestion et la sécurisation des flottes d'équipements mobiles,*
- *la consultation et l'analyse automatiques des traces d'évènements du SI,*
- *etc.*

T4-5.1 Gérer les mots de passe pour qu'ils présentent une robustesse appropriée

Les mots de passe constituent un moyen simple et peu coûteux d'assurer un niveau minimal d'authentification des utilisateurs. Associé à l'identifiant de l'utilisateur, c'est un moyen d'authentification « mono facteur », qui se base sur « ce que l'utilisateur sait ».
Pour que ce moyen soit efficace, il est indispensable que « ce que l'utilisateur sait » ne puisse pas être deviné par une autre personne. Des règles et conseils doivent ainsi être communiqués aux utilisateurs pour qu'ils construisent des mots de passe qui leur soient faciles à mémoriser, tout en restant suffisamment complexes pour ne pas être devinés ou construits par une personne qui voudrait usurper leur identité.

Exemple de mot de passe	
Mot de passe non robuste	Mot de passe robuste
28011968 Date de naissance	**1Ax5b=5Ab!** Mot de passe robuste et mémorisable

Exigences :

⇒ Une règle doit définir les conditions auxquelles doit répondre tout mot de passe pour être considéré comme robuste. Elle doit également définir, par dérogation, les critères dégradés acceptés pour certains dispositifs, spécifiques et identifiés, qui ne peuvent gérer les mots de passe définis selon la règle générale (ex. code « pin » exclusivement numérique pour une carte à puce, un ordiphone, un téléphone IP, une imprimante/scanner, le déverrouillage du poste téléphonique ou l'accès à la messagerie téléphonique).

⇒ Les utilisateurs doivent être formés à la nécessité d'utiliser des mots de passe robustes, à la façon de construire ces mots de passe robustes et néanmoins mémorisables et aux mauvaises pratiques à éviter dans ce domaine.
⇒ Les utilisateurs doivent être encouragés à utiliser des mots de passe différents pour des usages différents (par exemple par type d'usage ou par niveau de sensibilité), afin notamment que la compromission d'un de leurs mots de passe ne mette pas à mal l'ensemble des accès dont ils disposent.
⇒ Un renouvellement régulier des mots de passe doit être imposé aux utilisateurs. La périodicité du renouvellement doit être fixée en fonction du niveau de confiance souhaité dans l'opération d'authentification, de la robustesse *a priori* des mots de passe au vu des règles de constitution imposées et de la facilité de l'opération de changement du mot de passe par l'utilisateur. Dans tous les cas, tout mot de passe doit être renouvelé au moins annuellement.
⇒ Des mesures doivent être mises en place pour garantir qu'à tout moment les mots de passe configurés sont conformes aux règles de constitution des mots de passe et connus du seul titulaire du compte associé.
⇒ Quand c'est possible, des mesures doivent être mises en œuvre afin de vérifier la robustesse effective des mots de passe configurés.
⇒ Les dispositifs ne doivent jamais stocker les mots de passe « en clair », ni sous une forme qui permette à un tiers de retrouver le mot de passe ou de s'authentifier à la place de l'utilisateur légitime par une méthode détournée.

Déclinaison en règles :

Règles sur la gestion des mots de passe :

Réf.	Règles	Catégories de moyens du SI concernées
4.5.1.1	Les règles de constitution des mots de passe doivent être établies et communiquées aux utilisateurs. Les mots de passe doivent : • Avoir une longueur d'au moins 9 caractères ; • Avoir une longueur d'au plus 24 caractères ; • Etre constitués de caractères de quatre types : lettres majuscules, lettres minuscules, chiffres et caractères « spéciaux » (ponctuation, parenthèses, dièse, pourcent, …) ; • Contenir au moins un caractère de chaque type mentionné ci-dessus ; • Etre différents des trois derniers mots de passe utilisés.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.2	Une règle aussi peu dégradée que possible devrait être explicitement définie pour la constitution des mots de passe sur les systèmes qui ne supportent pas l'ensemble des règles énoncées précédemment.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.3	Des actions initiales et récurrentes de formation des utilisateurs aux règles de constitution des mots de passe doivent être organisées. Ces actions doivent également leur proposer des moyens simples de constituer des mots de passe robustes et conformes aux règles.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.4	Les utilisateurs doivent être formés à ne pas conserver leur mot de passe « en clair » ni utiliser d'information	*Equipements d'infrastructure système et réseau,*

	« publique » pour constituer leurs mots de passe, telles que : • Mots du dictionnaire (quelle qu'en soit la langue) • Prénoms • Nom avec lesquels ils ont un lien (nom d'un proche, de leur lieu de résidence, nom ou sigle de l'établissement, nom du fournisseur apposé sur un équipement présent à côté d'eux ou sur un panneau en face de la fenêtre de leur bureau, …) • Leur date de naissance ou celle d'un proche, date de mariage... (notamment pour les codes PIN) • Immatriculation de leur véhicule • Etc.	*Equipements utilisateurs*
4.5.1.5	Des règles de renouvellement de mot de passe doivent être définies et leur bonne application imposée par les systèmes, ou à défaut vérifiée par le personnel en charge de la SSI. Ces règles peuvent être modulées en fonction du contexte. Par exemple : • Pour un système où le respect de la règle de robustesse est assuré, renouvellement trimestriel ; • Pour un système sensible qui ne peut garantir le respect de la règle de robustesse, renouvellement mensuel ; • Pour un système sans sensibilité particulière et pour lequel le changement de mot de passe est lourd à réaliser, renouvellement semestriel. Ces règles concernent l'ensemble des équipements du SI, y compris les téléphones fixes ou mobiles, la messagerie vocale, les digicodes d'accès aux locaux, les codes d'accès aux imprimantes… Une décision doit être prise après analyse des enjeux dans le cas où des contraintes contradictoires du point de vue sécurité apparaissent, par exemple un système sensible qui ne permet pas de garantir des mots de passe robustes et dont le changement des mots de passe est laborieux pour les utilisateurs. Dans un tel cas, une acceptation éclairée des risques qui découlent éventuellement de la décision doit être formalisée par le responsable métier concerné.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.6	Tout dispositif qui supporte cette fonctionnalité devrait être paramétré pour que, lors du changement de mot de passe par l'utilisateur, tout mot de passe non conforme à la règle de constitution soit refusé.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.7	Tout dispositif qui supporte cette fonctionnalité devrait être paramétré pour que, lors du changement de mot de passe par l'utilisateur, tout mot de passe identique à l'un des trois mots de passe précédemment utilisés soit refusé.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

4.5.1.8	Le mot de passe initial, attribué au titulaire d'un compte nouvellement créé sur un dispositif ou suite à l'oubli ou l'annulation d'un mot de passe, doit être généré aléatoirement à chaque fois et se conformer à la règle de constitution des mots de passe. Ce mot de passe doit être changé par l'utilisateur dès sa première authentification.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.9	Une procédure récurrente, par exemple mensuelle, de vérification de la qualité des mots de passe devrait être mise en place afin de détecter les mots de passe trop « faibles » qu'une personne mal intentionnée pourrait trouver à l'aide d'outils spécialisés. Cette charge de doit être exécutée par un groupe restreint de personnes de confiance, typiquement des membres de l'équipe en charge de la SSI, à l'aide des mêmes outils librement disponibles que ceux utilisables par des personnes malveillantes. Ces outils doivent rechercher les mots de passe pendant une durée donnée, par exemple 24h et produire la liste des utilisateurs pour lesquels le mot de passe a été trouvé dans ce délai (avec le cas échéant le délai utilisateur par utilisateur). Cette liste doit rester strictement confidentielle et chaque utilisateur doit être informé individuellement et discrètement de la nécessité de changer immédiatement son mot de passe, avec pédagogie et en lui rappelant les règles et conseils associés. A aucun moment les mots de passe trouvés ne doivent être affichés ou stockés de quelque manière que ce soit.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.1.10	Les dispositifs techniques qui constituent le SI ne doivent jamais stocker ou transmettre de mots de passe « en clair », ni sous une forme qui permette à un tiers de retrouver le mot de passe ou de s'authentifier à la place de son détenteur légitime par une méthode détournée.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

Le site Internet https://www.ssi.gouv.fr/entreprise/guide/mot-de-passe/ propose une fiche technique sur les mots de passe, qui énonce également un ensemble de règles et de conseils sur ce thème.

Des outils qui permettent aux utilisateurs de conserver de manière sécurisée leurs différents mots de passe (« trousseau » ou « portefeuille » de mots de passe) sont référencés sur le site de l'ANSSI (www.ssi.gouv.fr).

T4-5.2 Verrouiller les postes de travail

Une session de travail laissée accessible sur un poste de travail en l'absence de son utilisateur peut permettre à une personne malveillante d'usurper l'identité de l'utilisateur en utilisant son poste, d'accéder à des informations qui ne lui sont pas autorisées, voire de porter atteinte à la sécurité du SI sans laisser de trace qui permette de l'identifier. Il est nécessaire que les utilisateurs se prémunissent contre ce genre de menace susceptible de les affecter personnellement (puisque c'est sous

leur identité que des actions malveillantes peuvent être menées dans ce cas) en plus d'affecter la structure.

Exigence :

⇒ Quand un utilisateur s'est authentifié sur un équipement du SI, il doit soit se déconnecter, soit verrouiller sa session d'utilisation quand il s'éloigne de cet équipement au point de ne plus pouvoir contrôler à tout instant qui y accède.

Déclinaison en règles :

Règles sur le verrouillage des postes de travail :

Réf.	Règles	Catégories de moyens du SI concernées
4.5.2.1	Les utilisateurs doivent être sensibilisés à la protection des équipements du SI qui leur sont confiés, afin qu'ils prennent l'habitude de se déconnecter ou de les verrouiller quand ils s'absentent. Ces principes doivent être appliqués avec une plus grande attention quand les règles 3.1.2.1 et 3.1.2.2 de l'organisation des locaux ne peuvent pas être intégralement respectées.	*Equipements utilisateurs/Terminaux*
4.5.2.2	Si un moyen matériel (carte à puce ou autre) est utilisé pour l'authentification des utilisateurs sur leur poste, son extraction du poste doit entraîner le verrouillage immédiat du poste ou la déconnexion logique de l'utilisateur. Les utilisateurs doivent alors prendre l'habitude de toujours garder leur carte avec eux et de la retirer du lecteur quand ils s'absentent. L'utilisation de cette même carte pour le contrôle d'accès physique aux locaux et parkings ainsi que le self ou le télétravail renforce cette prise d'habitude.	*Equipements utilisateurs/Terminaux*
4.5.2.3	Le verrouillage automatique des postes de travail après une durée d'inactivité compatible avec les activités des utilisateurs, éventuellement couplé à une mise en veille, devrait être activé. Le paramétrage d'une durée d'inactivité de 20 minutes est généralement adapté.	*Equipements utilisateurs/Terminaux*
4.5.2.4	Les postes de travail devraient être paramétrés pour qu'à leur sortie de veille ou à la sortie de veille de leur écran, ils soient verrouillés et imposent à l'utilisateur de s'authentifier à nouveau.	*Equipements utilisateurs/Terminaux*

T4-5.3 Assurer la protection logique des équipements informatiques

Les défauts inhérents à tout logiciel sont susceptibles d'être exploités pour porter atteinte à la sécurité du SI. Des mesures doivent être mises en œuvre afin de limiter l'exposition à ces vulnérabilités et de restreindre leurs impacts tant qu'elles ne sont pas corrigées.

Exigences :

⇒ Un dispositif de détection et de blocage de logiciels malveillants doit être mis en œuvre et maintenu à jour sur tout équipement qui supporte cette fonctionnalité.

⇒ Des dispositifs doivent être mis en œuvre pour garantir que seules les communications légitimes sont autorisées entre les différents équipements connectés au SI.

⇒ Les privilèges dont disposent les utilisateurs sur les équipements auxquels ils ont accès ne doivent pas excéder leurs besoins usuels. Si des privilèges supérieurs leur sont ponctuellement et légitimement nécessaires, ils ne doivent leur être accordés que de façon temporaire. Cette opération peut être effectuée par l'utilisateur lui-même, par exemple par l'usage d'un deuxième compte utilisateur, privilégié, qui lui est attribué, ou par une commande qui permet une élévation temporaire de privilèges après authentification.

⇒ Les services qui sont proposés par les systèmes d'exploitation, applications ou équipements, mais qui ne sont pas nécessaires à l'utilisation prévue, doivent être désactivés et si possible ne pas être installés du tout.

Déclinaison en règles :

Règles sur la protection logique des équipements :

Réf.	Règles	Catégories de moyens du SI concernées
4.5.3.1	Tout poste de travail fixe ou mobile, ordiphone ou tablette devrait disposer d'un logiciel antivirus.	*Equipements utilisateurs/Terminaux*
4.5.3.2	Tout serveur, quel que soit son système d'exploitation, qui stocke ou par lequel peuvent transiter des contenus dans des formats susceptible de cacher des logiciels malveillants, doit disposer d'un logiciel antivirus. Il est recommandé que l'antivirus utilisé pour les serveurs soit différent de celui utilisé pour les postes de travail. Les formats susceptibles d'héberger des logiciels malveillants et pris en compte par les antivirus du marché sont notamment : • L'ensemble des logiciels pour plateformes Microsoft ; • L'ensemble des fichiers bureautiques (traitement de texte, présentation, tableur, …); • Les fichiers PDF ; • Les fichiers images et vidéo ; • Les fichiers « archives » (.zip, .rar, .tar…) • Les fichiers en langage de « script » de toutes natures (batch, javascript, …)	*Equipements d'infrastructure système et réseau/Serveurs*
4.5.3.3	L'antivirus de chaque équipement devrait être paramétré pour se mettre à jour sans intervention de l'utilisateur avec une périodicité au moins journalière. Les équipements qui ne sont pas connectés en permanence au réseau doivent mettre à jour leur antivirus dès qu'ils sont connectés.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.4	Une procédure et si possible un moyen automatisé tel qu'une plateforme de gestion centralisée, doivent garantir qu'un antivirus est effectivement installé, activé et à jour sur tout équipement qui doit en être doté.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

4.5.3.5	Le personnel informatique doit être alerté en cas d'anomalie de présence, d'activité ou de mise à jour d'antivirus, ainsi qu'en cas de détection de fichier potentiellement malveillant sur un équipement.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.6	L'état d'activation et de mise à jour de l'antivirus doit être clairement visible de l'utilisateur, qui doit pouvoir déclencher manuellement une mise à jour s'il le considère nécessaire.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.7	Les utilisateurs devraient être sensibilisés à l'importance de la présence d'un antivirus actif et à jour sur leur poste de travail. Ils doivent être encouragés à en vérifier occasionnellement l'état (et ce d'autant plus si une vérification centralisée automatique n'est pas possible).	*Equipements utilisateurs/Terminaux*
4.5.3.8	Tout équipement qui supporte cette fonctionnalité (serveur, poste de travail, certains ordiphones, tablettes) devrait disposer d'un système pare-feu activé et paramétré pour limiter strictement les échanges réseau aux flux nécessaires. Dans la plupart des environnements, les seuls échanges réseau utiles qui impliquent les postes de travail ou les imprimantes sont réalisés avec les serveurs. Dès lors, si le réseau est correctement structuré, il est possible d'interdire, à l'aide du pare-feu du poste, tout flux entre le poste et les adresses réseau qui ne sont pas susceptibles d'appartenir à un serveur. Cette mesure restreint considérablement les possibilités de propagation d'activités malveillantes ou non prévues entre les postes de travail, tout en facilitant la détection de flux anormaux entre deux points qui ne devraient pas être en mesure de communiquer (révélant par exemple un poste connecté illicitement, voire en train de réaliser une exploration du réseau pour préparer une action malveillante).	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.9	Les serveurs de messagerie, postes de travail, ordiphones et tablettes devraient disposer d'une fonction anti-spam activée et mise à jour selon les mêmes principes que pour l'antivirus.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.10	Les serveurs applicatifs les plus sensibles, devraient, quand le mode de fonctionnement des applications le permet, n'être accessible que via des dispositifs relais ou « reverse proxy », qui assurent une vérification des échanges du point de vue protocolaire et qui intègrent une détection et un blocage automatique des contenus potentiellement malveillants, L'utilisation d'un « reverse proxy », qui peut être mutualisé entre plusieurs services ouverts sur Internet, est particulièrement importante pour détecter et bloquer des vulnérabilités « génériques » potentiellement présentes, notamment pour les applications web. Elle permet aussi, en cas de	*Equipements d'infrastructure système et réseau/Serveurs*

	vulnérabilité identifiée, de mettre rapidement en place des mesures de protection, dans l'attente de l'installation d'un correctif spécifique à l'application.	
4.5.3.11	Quel que soit le type d'équipement (poste de travail, serveur, équipement biomédical, téléphone mobile, imprimante, scanner, autocommutateur, routeur…), seuls les logiciels et services et comptes effectivement nécessaires au bon fonctionnement des équipements et à l'activité prévue devraient être installés et activés. Les autres devraient être désinstallés si c'est possible (et de préférence ne jamais être installés), ou à défaut être désactivés. De la même manière, les ports de communication des équipements (ports réseau de routeurs, de commutateurs, de serveurs, interface sans fil de poste de travail : Wifi, Bluetooth, 3G …) devraient être désactivés s'il n'est pas prévu qu'ils soient utilisés.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.12	Les navigateurs Internet installés sur les postes de travail, voire sur les serveurs, qui le nécessitent, doivent être configurés afin de renforcer leur sécurité, conformément aux bonnes pratiques en vigueur. L'ANSSI publie des recommandations pour le déploiement sécurisé de différents types de navigateurs Internet : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/poste-de-travail-et-serveurs	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.13	Une procédure formalisée de configuration devrait être établie pour chaque type de composant du SI afin de garantir l'homogénéité des configurations et la bonne sécurisation des postes de travail, serveurs, équipements réseau, applications... Les structures qui relèvent du secteur public doivent se conformer aux directives nationales ou ministérielles relatives à la configuration des équipements informatiques. L'ANSSI publie des recommandations pour la sécurisation des postes de travail et des serveurs : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/poste-de-travail-et-serveurs	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
4.5.3.14	Outre les autres règles de T4-5.3, la sécurisation des imprimantes simples ou multifonctions devrait prévoir l'activation du chiffrement des données sur son disque dur quand cette fonction est disponible.	*Equipements utilisateurs/Terminaux (ex. Imprimantes)*
4.5.3.15	Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi uniquement à une seule adresse de messagerie.	*Equipements utilisateurs/Terminaux*
4.5.3.16	Outre les autres règles de T4-5.3, la sécurisation des autocommutateurs devrait être assurée comme pour tout composant du SI, avec notamment : • maintient à jour des correctifs de sécurité ; • sécurisation spécifique de la configuration selon le modèle d'autocommutateur ;	*Equipements d'infrastructure système et réseau/Téléphonie*

	• définition et affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) réalisée avec une attention particulière ; • revue de la programmation téléphonique organisée périodiquement. La problématique de sécurisation des autocommutateurs est loin d'être anecdotique : les piratages de systèmes téléphoniques d'organismes privés ou publiques sont fréquents. Leur détournement au profit d'organisations criminelles est l'un des moyens qui permet à certains « opérateurs » peu scrupuleux de fournir des communications internationales à bas coût : en effet, c'est l'organisme piraté qui paie les communications qui transitent par son autocommutateur, et la facture s'élève souvent à plusieurs milliers d'Euros avant qu'il ne découvre le problème…	
4.5.3.17	L'usage de privilèges « administrateur » sur les équipements (postes de travail notamment) doit être limité au strict nécessaire. Sur les systèmes informatiques où le changement fréquent de niveau de privilège n'est pas possible ou se fait de manière peu naturelle (certains systèmes Windows par exemple), seuls les administrateurs systèmes à plein temps doivent pouvoir disposer d'un compte principal qui possède le privilège « administrateur ». Sur les systèmes informatiques où le changement de niveau de privilège est simple (systèmes de la famille Unix, Linux… par exemple), ou pour une utilisation qui ne nécessite que ponctuellement le privilège « administrateur » (ex. utilisateur assurant ponctuellement des fonctions d'administration système, développeur, …), il convient de favoriser l'utilisation d'un compte principal sans privilège particulier et d'un compte secondaire privilégié qui permet de lancer ponctuellement des commandes en mode administrateur à l'aide de fonctionnalités telles que « exécuter en tant que… ». Le périmètre d'action des privilèges administrateurs doit être restreint au strict nécessaire (ex. dans le cas du compte secondaire privilégié d'un développeur, le périmètre des droits administrateur doit se limiter à son seul poste de travail et non pas s'étendre à l'ensemble du SI). Des privilèges « administrateur » sont parfois nécessaires à l'usage de certains logiciels, notamment dans le cadre de développement logiciel ou de tests de paramétrage ou d'intégration du SI. Une solution souvent pertinente consiste à réaliser ces opérations dans un environnement virtualisé	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

	(« machine virtuelle »). L'utilisateur peut alors disposer de droits « administrateurs » dans cet environnement « poste de travail virtuel », sans les nécessiter pour son poste de travail réel.	
4.5.3.18	Il est recommandé que les postes de travail utilisés principalement pour des tâches d'administration de composant informatiques du SI (serveurs, équipements réseau, antivirus…) : • soient dédiés à cette fonction ; • soient rassemblés dans un local à accès restreint et dédié à l'administration du SI ; • bénéficient de mesures de sécurité renforcées (fréquence des mises à jour d'antivirus plus élevée, surveillance approfondie des traces d'anomalies enregistrées…) ; • intègrent un dispositif de machine virtuelle (voir note en fin de 4.5.3.17), également sécurisée et utilisée spécifiquement pour accéder à Internet, cette mesure permettant d'isoler l'environnement exposé aux menaces Internet du poste de travail d'administration qui lui dispose d'accès privilégiés aux composants du SI.	*Equipements utilisateurs/Terminaux*
4.5.3.19	Le partage de répertoires ou de données hébergées localement sur les postes de travail devrait être interdit. Les données qui nécessitent d'être accessibles depuis plusieurs postes ou équipement doivent résider sur un serveur. Dans les structures dont le SI ne comporte que quelques postes, il peut être tentant de partager directement les données entre les postes de travail. Pourtant, cette pratique met en risque la préservation et la protection des données : on constate souvent que, rapidement, le contrôle d'accès est trop permissif (données sensibles accessibles à tous depuis le réseau local), que les répertoires contenant les données se multiplient et sont mal identifiés, que l'ensemble des données n'est pas sauvegardé comme escompté, que des données partagées sont perdues lors du remplacement d'un des postes tombé en panne… La mise en place d'un serveur de fichier permet une maîtrise du stockage des données et une centralisation de leur protection (contrôle d'accès, dispositifs palliant aux défaillances des disques de stockage, sauvegarde simplifiée) pour un surcoût limité.	*Equipements utilisateurs/Terminaux*
4.5.3.20	Si un système de messagerie « technique » est mis en œuvre pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, ou pour remplir des fonctions de messagerie inter-applicative (« machine à machine »), elle ne doit être en aucun cas accessible aux utilisateurs (sauf accès par les administrateurs du SI habilités).	*Equipements d'infrastructure système et réseau*

4.5.3.21	Le choix des outils de sécurité utilisés pour sécuriser les équipements informatiques doit respecter la règle 6.5.1.9.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T4-5.4 Vérifier l'authenticité des logiciels

On peut vérifier l'authenticité d'un logiciel si on est en mesure de garantir qu'il provient bien d'une source identifiée de confiance (industriel, site Internet renommé…) et qu'il est absolument identique à la version diffusée par cette source. La présence au sein du SI de logiciels dont il n'est pas possible de garantir cette authenticité soulève trois risques principaux :

- Un premier risque de sécurité : modification malveillante d'un logiciel initialement issu d'une source de confiance afin, par exemple, de permettre ultérieurement une prise de contrôle à distance de composants du SI ;
- Un deuxième risque de sécurité, proche mais distincte du premier : logiciel issu d'une source non identifiée ou non fiable, qui intègre les mêmes fonctionnalités malveillantes dissimulées que dans le premier cas, sous couvert des fonctionnalités pratiques ou agréables à l'utilisateur utilisées comme « appât » ;
- Un risque légal : logiciel dont la source n'a pas été identifiée et dont l'utilisation est faite sans la rétribution nécessaire (absence de licence…).

Exigences :

⇒ Pour tout logiciel installé, quels que soient les moyens employés pour son obtention et son installation, l'origine du logiciel doit être identifiée et le moyen de vérifier son authenticité doit être documentée.

⇒ L'authenticité de tout logiciel doit être vérifiée avant son installation sur les équipements du SI.

⇒ Pour les composants les plus sensibles du SI, une vérification formalisée de l'authenticité des logiciels installés doit être réalisée régulièrement et au moins de façon annuelle.

Déclinaison en règles :

Règles sur la vérification de l'authenticité des logiciels :

Réf.	Règles	Catégories de moyens du SI concernées
4.5.4.1	L'installation de logiciels doit se faire à l'aide des supports originaux (CD, DVD) tels qu'obtenus du fournisseur, à l'exclusion de toute copie et présentant les caractéristiques visuelles attendues quand l'éditeur prévoit une telle disposition (ex. image holographique pour les supports des logiciels Microsoft).	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
4.5.4.2	Quand le logiciel est téléchargé depuis Internet, qu'il ait été acheté ou qu'il soit gratuit, l'authenticité du site d'obtention et de téléchargement doit être vérifiée : l'accès doit utiliser le protocole HTTPS et le certificat de sécurité présenté par le site web doit être valide et cohérent avec les attentes (nom du titulaire du certificat, autorité de certification connue…).	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

4.5.4.3	Quand le logiciel est téléchargé depuis Internet, des sommes de contrôle (MD5, SHA) sont parfois publiées (généralement pour les logiciels libres) et devraient alors être utilisées pour vérifier l'intégrité des logiciels obtenus.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
4.5.4.4	Certains systèmes d'exploitation (versions récentes des systèmes Microsoft, nombreuses distributions Linux) mettent en œuvre des dispositifs de vérification automatique et systématique de l'authenticité des logiciels au moment de leur installation via les outils prévus par le système ou lors de leur mise à jour. Une alerte de défaut d'authenticité devrait être rédhibitoire pour l'installation. Une alerte d'absence de possibilité de vérification devrait être prise en compte avec le plus grand sérieux et, dans le doute, aboutir à l'abandon de l'installation du logiciel.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
4.5.4.5	Si des logiciels destinés à être installés sont stockés sur un « serveur d'installation », un dispositif de contrôle d'intégrité de ces logiciels devrait être mis en œuvre afin de garantir qu'ils ne sont pas modifiés entre le moment où ils sont déposés sur le serveur et celui où ils sont utilisés pour des installation effectives.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

T4-5.5 Procéder à une mise à niveau régulière des moyens informatiques

Pour les mêmes raisons que celles qui justifient la mise en œuvre de protections logiques des équipements informatiques, une mise à jour régulière des logiciels systèmes et applicatifs des moyens informatiques doit être organisée. Outre le traitement préventif de dysfonctionnements potentiels, ce principe permet d'éviter que des défauts publiquement connus puissent être utilisés pour porter atteinte à la sécurité du SI.

Exigences :

⇒ Les équipements et logiciels doivent être maintenus et mis à jour en cohérence avec la mise à disposition des mises à jour et des correctifs de sécurité par les industriels.

⇒ Le remplacement des équipements et logiciels dont la fin de période de maintenance approche doit être anticipée et planifiée.

Déclinaison en règles :

Règles sur la mise à niveau des moyens informatiques :

Réf.	Règles	Catégories de moyens du SI concernées
4.5.5.1	Une procédure qui garantit la mise à jour régulière de chaque logiciel du parc informatique devrait être mise en place. Cette procédure doit prendre en compte les spécificités éventuelles de certains composants du SI (systèmes exposés à Internet qui requièrent des mises à jour dans de brefs délais, équipements utilisés 24h/24 dont les interruptions doivent être rares et courtes…) Dans les environnements informatiques simples, pour les équipements qui disposent d'une configuration de logiciels standard, une mise à jour automatisée doit être favorisée chaque fois que possible.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

	Dans les cas de parcs informatiques importants ou d'équipements qui hébergent des logiciels multiples et hétérogènes et notamment si des risques d'incompatibilités entre logiciels sont identifiés, il est recommandé que la mise à jour soit réalisée sur une plateforme de validation avant déploiement en environnement de production.	
4.5.5.2	Les correctifs de sécurité doivent impérativement être appliqués, à moins : • qu'il ne soit démontré que les vulnérabilités corrigées par ce correctif ne peuvent être exploitées d'aucune façon dans ce contexte particulier ; • ou que le responsable métier de l'équipement concerné comprenne pleinement et accepte les risques induits par l'existence des vulnérabilités qui devaient être traitées par le correctif et que le responsable de la SSI vérifie que la persistance de ces vulnérabilités non corrigées sur l'équipement ne peut en aucun cas induire des risques supplémentaires pour le reste du SI.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
4.5.5.3	Une attention particulière devrait être portée à l'identification de la date de fin de maintenance d'un logiciel ou d'un équipement par l'industriel. Le composant doit être remplacé par un autre maintenu par un industriel avant cette échéance.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
4.5.5.4	L'absence de mise à disposition régulière de correctif ou mise à niveau des logiciels d'un équipement informatisé de quelque type que ce soit devrait déclencher une action à l'égard de ce fournisseur, soit pour obtenir les dernières mises à jour, soit pour envisager de changer de fournisseur, en fonction des risques qui ont été identifiés en lien avec la non mise à jour.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
4.5.5.5	Tout système qui présente des failles de sécurité ne pouvant être corrigées du fait de l'absence de mise à jour applicable et qui ne peut être remplacé devrait être isolé du reste du SI : • si les données stockées ou les traitements réalisés par ce système sont sensibles et se trouvent exposés à un risque inacceptable du fait de la faille non corrigée (*ex : des informations de santé de patient sont accessible librement via le réseau local par tout personnel interne qui connaît la méthode pour y accéder)* ; • ou si les systèmes qui l'environnent se trouvent eux-mêmes mis à risque du fait de cette faille non corrigée *(ex : un système qui télécharge automatiquement ses mises à jour depuis Internet authentifie le site de téléchargement à l'aide d'un certificat dont on sait qu'il a été*	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

	compromis. Dès lors, les mises à jours sont potentiellement téléchargées depuis un site malveillant qui usurpe l'identité du site légitime et qui pourrait utiliser ce moyen pour prendre le contrôle de ce système, et de là pirater le reste du SI via le réseau local) Cet isolement peut être réalisé en positionnant le système concerné sur une partie du réseau dédiée et cloisonnée du reste du SI, selon les principes exposés au T4-2.2, ou derrière un relai applicatif tel que requis par 4.5.3.10. Afin de ne pas compromettre les comptes utilisés dans le reste du SI, il peut être nécessaire de mettre en place des comptes (administrateurs, utilisateurs) et des moyens d'authentification spécifiques à ce système.	

T4-5.6 Assurer la protection logique des supports informatiques et équipements mobiles (smartphone, tablettes, …) qui contiennent des données sensibles (dont les données de santé à caractère personnel)

Les supports de données amovibles (clés USB, disque dur externe, CD-Rom, …) et les terminaux mobiles sont des composants du SI particulièrement vulnérables du point de vue de la SSI :

- Par leur nature même (amovibles, légers, de petite taille, utilisés en des lieux multiples), ils peuvent très facilement être perdus ou volés ;
- Du fait de leur utilisation fréquente et perçue comme facilitatrice des activités, les utilisateurs sont peu enclins à leur ajouter des fonctions de sécurité qui apparaissent comme des freins à la souplesse d'usage ;
- Les équipements mobiles sont souvent diffusés par les industriels dans une logique d'équipement personnel qui permet à l'utilisateur d'installer tout logiciel qu'il souhaite, parmi lesquels peuvent se cacher des logiciels malveillants.

Ces différents points exposent les données de santé à caractère personnel et les autres données sensibles à de nombreux risques quand elles sont stockées sur de tels équipements.

Exigences :

⇒ Des règles doivent être établies pour le suivi et la protection spécifique des supports de données amovibles et des terminaux mobiles qui contiennent des données sensibles.
⇒ Les utilisateurs doivent être sensibilisés à ces règles et mobilisés pour leur application active.
⇒ L'usage de ces équipements à l'extérieur de l'établissement doit être réduit au strict nécessaire et doit donner lieu à un suivi.
⇒ Les solutions de sécurité additionnelles disponibles pour les équipements concernés doivent être mises en œuvre : chiffrement des données, maîtrise des logiciels installés et de la configuration sur les terminaux mobiles, antivirus…
⇒ Les fonctions qui ne sont pas nécessaires à l'activité sur les terminaux mobiles doivent être désactivées.

Déclinaison en règles :

Règles sur la protection logique des supports de données amovibles et des équipements mobiles :

Réf.	Règles	Catégories de moyens du SI concernées
4.5.6.1	Un équipement mobile (ordiphones, tablettes, ordinateur portable) ne devrait être autorisé à stocker des données sensibles ou à se connecter au SI que s'il intègre les fonctions de sécurité suivantes, de façon native ou grâce à des logiciels additionnels : • antivirus ; • maîtrise par les services informatiques de la configuration de l'équipement et des logiciels installés ; • pare-feu.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette)*
4.5.6.2	Un équipement mobile ne devrait être autorisé à stocker des données sensibles que si : • il intègre une fonction de chiffrement des données, de façon native ou grâce à un logiciel additionnel ; • et que cette fonction est effectivement appliquée aux données sensibles.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette)*
4.5.6.3	Tout service ou fonction qui n'est pas nécessaire à l'activité prévue sur l'équipement mobile devrait être désinstallé, ou à défaut désactivé, ou si ce n'est pas possible, bloqué par le pare-feu. En outre, les utilisateurs devraient être formés à n'activer les interfaces de communication sans fil (Wifi, Bluetooth, 3G, 4G…) que pendant les périodes où ils les utilisent effectivement.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette)*
4.5.6.4	Les données sensibles stockées sur un support de données mobile (clés USB, disque dur externe ou amovible…) devraient être chiffrées.	*Equipements utilisateurs/Support de données amovible (ex. clés USB)*
4.5.6.5	Le choix des outils de sécurité utilisés pour sécuriser les supports informatiques et les équipements mobiles devrait respecter la règle 6.5.1.9.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette), Equipements utilisateurs/Support de données amovible (ex. clés USB)*
4.5.6.6	Sauf dérogation, il devrait être interdit de transporter des données sensibles (et en particulier des données de santé à caractère personnel) à l'extérieur de l'établissement ou d'utiliser un terminal mobile qui contient de telles données à l'extérieur de l'établissement.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette), Equipements utilisateurs/Support de données amovible (ex. clés USB)*
4.5.6.7	Une procédure devrait définir les modalités de délivrance des autorisations dérogatoires de transport des données sensibles à l'extérieur de l'établissement d'une part, et d'utilisation à l'extérieur de l'établissement d'un terminal mobile qui contient de telles données d'autre part, les conditions à respecter, le responsable qui les délivre et la revue au moins annuelle de ces dérogations.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette), Equipements utilisateurs/Support de données amovible (ex. clés USB)*

4.5.6.8	L'autorisation dérogatoire de transport des données sensibles, ou d'utilisation d'un terminal mobile qui contient de telles données, à l'extérieur de l'établissement devrait être donnée sous condition d'utilisation de supports de données sécurisés, explicitement identifiés et attribués nominativement au bénéficiaire de l'autorisation qui doit en assumer la responsabilité de la protection. Ces supports doivent être retournés au responsable à l'échéance de la dérogation.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette), Equipements utilisateurs/Support de données amovible (ex. clés USB)*
4.5.6.9	Les utilisateurs du SI devraient être informés des règles relatives aux transports de données sensibles (et en particulier de données de santé à caractère personnel) à l'extérieur de l'établissement et d'usage de terminaux mobiles à l'extérieur de l'établissement.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette), Equipements utilisateurs/Support de données amovible (ex. clés USB)*
4.5.6.10	Les autorisations de stockage d'informations sur une équipement mobile ou un support de données amovible, les autorisations dérogatoire de transport de données sensibles à l'extérieur de l'établissement et les autorisations dérogatoire d'utilisation de terminaux mobiles à l'extérieur de l'établissement devraient être délivrées exclusivement par l'autorité d'homologation, soit sur une base individuelle, soit sur une base de critères et de conditions que cette autorité établit et formalise conformément à 4.5.6.7.	*Equipements utilisateurs/Terminaux (ex. ordinateur portable, tablette), Equipements utilisateurs/Support de données amovible (ex. clés USB)*

Thématique 5 : Maîtriser les accès aux informations

T5-1 Accorder les accès aux informations aux seules personnes dûment autorisées

T5-1.1 Formaliser des règles d'accès aux informations

Exigence :

⇒ Les droits d'accès définis pour le système d'information doivent assurer que les informations ne sont accessibles qu'aux personnes en ayant besoin pour leurs tâches professionnelles.

Déclinaison en règles :

Règles sur la formalisation des règles d'accès aux informations en général :

Réf.	Règles	Catégories de moyens du SI concernées
5.1.1.1	Chaque application identifiée dans l'inventaire des moyens du SI doit mettre en œuvre des droits d'accès aux fonctionnalités applicatives et aux données basées sur le type d'utilisateur	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.1.2	Chaque application a au moins deux types d'utilisateur, qu'elle distingue à l'aide de profils applicatifs : • administrateur technique de l'application ; • utilisateur métier de l'application. Selon les fonctionnalités de l'application et la nécessité de restreindre l'accès aux informations, il peut y avoir plus d'un profil applicatif pour les utilisateurs métiers (ex. pour un logiciel médical, un type d'utilisateur « administratif » qui n'a pas accès aux données de santé à caractère personnel et un type d'utilisateur « professionnel de santé » qui a accès aux données de santé à caractère personnel). Les utilisateurs doivent, autant que possible, être associés aux profils applicatifs préconisés par les industriels en fonction de leur activité pour les logiciels concernés.	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.1.3	Une liste devra être élaborée et tenue à jour pour chaque logiciel et énumérer chaque profil applicatif défini dans le logiciel avec les données et les fonctions auxquelles il peut accéder.	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.1.4	Des profils utilisateurs devraient être élaborés et correspondre aux types de fonctions métier assurées par les personnels de la structure et les personnes extérieures ayant vocation à accéder au système d'information (ex. prestataire). Un profil utilisateur liste, pour un type de fonction métier donné, l'ensemble des applications auxquelles la personne remplissant cette fonction a accès et les profils applicatifs associés à cette fonction métier dans chaque application. La logique d'élaboration d'un profil utilisateur est : • de ne donner l'accès qu'aux applications nécessaires à l'exécution des tâches associées à la fonction ;	*Equipements d'infrastructure système et réseaux - logiciels*

	• d'y associer le profil applicatif disposant le moins de droits d'accès possibles mais suffisamment pour réaliser les tâches associées à la fonction ; • de ne pas mixer des droits de type administrateur technique et des droits de type utilisateur métier ; • si la taille de la structure le permet, d'interdire qu'un même profil utilisateur ait, via les profils applicatifs qui lui sont associés, tous les droits de type administrateur technique sur tous les logiciels. Il est nécessaire de différencier autant que possible les logiciels qui traitent d'informations sensibles (données à caractère personnel…) des autres logiciels.	
5.1.1.5	Une liste des profils utilisateurs avec les types de fonctions métier ainsi que les logiciels auxquels ils peuvent accéder et les profils applicatifs associés devra être élaborée et tenue à jour.	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.1.6	Les attributions de droits d'accès aux utilisateurs en accord avec le(s) profil(s) correspondant à leur(s) fonction(s) devraient être tracées. Ces traces doivent être aisément accessibles et compréhensibles sans expertise ou formation préalable particulière.	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.1.7	Les règles et procédures d'attribution de profils : • d'administrateur technique de composants du SI ou d'administrateur de composants de SSI ; • d'administrateur métier de composants du SI traitant d'informations sensibles ; • d'utilisateur de composants du SI traitant d'informations sensibles ; • d'administrateur métier ou d'utilisateurs de composants du SI ne traitant pas d'informations sensibles ; devraient être soumises à la validation de Commission habilitation.	*Catégories de personnel*
5.1.1.8	Les règles et procédures d'attribution de profils : • d'administrateur technique de composants du SI ou d'administrateur de composants de SSI ; • d'administrateur métier de composants du SI traitant d'informations sensibles ; devraient prévoir que la décision d'attribution du profil à un utilisateur soit soumise à la validation du Responsable de la SSI.	*Catégories de personnel*

Règles sur la formalisation des règles complémentaires pour l'accès aux données de santé à caractère personnel :

Réf.	Règles	Catégories de moyens du SI concernées
5.1.1.9	En fonctionnement nominal, seuls les personnels participant à la prise en charge sanitaire d'un usager peuvent avoir accès à ses informations de santé à caractère personnel.	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.1.10	De manière exceptionnelle, lorsqu'il est nécessaire d'accéder aux données au niveau technique (par exemple dans le cadre de la résolution d'un incident), l'accès à des informations de santé à caractère personnel doit se faire sous la responsabilité des personnes habilitées à intervenir sur les données de santé à caractère personnel en dehors de la prise en charge des usagers. Cet accès ne doit être accordé que de manière temporaire. Les raisons de cet accès exceptionnel, ainsi que les personnes en ayant bénéficié et la personne sous la responsabilité de laquelle il a été réalisé doivent être enregistrés et conservés au même titre que les autres éléments de traçabilité mis en œuvre par le système d'information tels que décrit dans le thème 7-2.	*Equipements d'infrastructure système et réseaux - logiciels*

T5-1.2 Gérer les accès aux informations

Exigence :

⇒ Les droits d'accès aux informations formalisés dans la PSSI doivent être mis en œuvre au niveau du système d'information.

Déclinaison en règles :

Règles sur la gestion des accès aux informations :

Réf.	Règles	Catégories de moyens du SI concernées
5.1.2.1	Chaque compte nominatif sur le système d'information doit mettre en œuvre un/des profil(s) utilisateur(s) définissant les applications auxquelles l'utilisateur à accès ainsi que les fonctionnalités applicatives qu'il peut utiliser et les données auxquelles il a accès. Cette association se fait à la prise de fonction de l'utilisateur tel que décrit dans le thème 2-2.2	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.2.2	Une liste ou un référentiel de l'ensemble des profils attribués à chaque compte du système devrait être élaboré et tenu à jour. Cette liste ou référentiel doit être tenu séparément du référentiel technique servant éventuellement de base aux opérations de contrôle d'accès logique au SI, afin de constituer une référence de vérification de la conformité de ce référentiel technique aux autorisations données.	*Equipements d'infrastructure système et réseaux - logiciels*
5.1.2.3	Chaque logiciel le permettant devrait être configuré pour restreindre l'accès aux informations et aux fonctions qui	*Equipements d'infrastructure*

	ne sont pas publiques aux seuls utilisateurs autorisés selon les principes définis au T5-1.1. De manière générale, l'accès aux données sensibles, à caractère personnel ou non, devrait être limité aux seules personnes habilitées à y accéder. En particulier, l'accès aux données de santé à caractère personnel d'un usager devrait être restreint aux seuls professionnels prenant en charge cet usager.	*système et réseaux - logiciels*
5.1.2.4	L'accès aux outils et interfaces d'administration du SI et de sa sécurité doit être strictement limité aux utilisateurs habilités et disposant des profils correspondants, selon les procédures fixées par les règles 5.1.1.7 et 5.1.1.8.	*Equipements d'infrastructure système et réseaux - logiciels*

T5-1.3 Contrôler régulièrement les droits d'accès

Exigence :

⇒ Les droits d'accès effectivement mis en œuvre doivent correspondre aux règles définies dans la PSSI pour l'accès aux données.

Déclinaison en règles :

Règles sur le contrôle des droits d'accès :

Réf.	Règles	Catégories de moyens du SI concernées
5.1.3.1	Le contrôle régulier des droits d'accès effectifs, tel que requis par les règles du thème T7-1.1, devrait vérifier la cohérence des quatre éléments suivants : • la liste des types de fonctions avec les profils utilisateurs et les droits d'accès qui y sont associés ; • la liste des utilisateurs et le/les profil(s) qui leur sont attribués ; • la liste des utilisateurs et des fonctions qu'ils occupent ; • la liste des droits effectivement mis en œuvre pour chaque utilisateur.	*Catégorie de personnel (ex. ensemble des utilisateurs et administrateurs du SI)*
5.1.3.2	Chaque contrôle des droits d'accès devrait porter sur : • l'ensemble des droits de type administrateur technique et des utilisateurs qui bénéficient de ces droits ; • un échantillon des droits de type utilisateur métier à changer à chaque contrôle.	*Catégorie de personnel*

T5-2 Adopter les bonnes pratiques en matière d'authentification des utilisateurs

T5-2.1 Créer des comptes qui respectent les bons usages

Exigence :

⇒ Les comptes utilisateurs sur le système d'information doivent être individuels et nominatifs.

Déclinaison en règles :

Règles sur le respect des bons usages en termes de comptes :

Réf.	Règles	Catégories de moyens du SI concernées
5.2.1.1	Chaque compte utilisateur doit être nominatif et uniquement utilisé par l'utilisateur auquel il est associé	*Catégorie de personnel (ex. ensemble des utilisateurs et administrateurs du SI)*
5.2.1.2	Si une personne est amenée à remplacer une autre personne et qu'elle a besoin de droits d'accès complémentaires pour ce faire, les profils utilisateurs en question devraient être temporairement attribués à son compte nominatif personnel. Elle ne doit en aucun cas utiliser le compte nominatif personnel de la personne remplacée.	*Catégorie de personnel*
5.2.1.3	Les comptes administrateurs techniques génériques par défaut des logiciels et des matériels ne devraient pas être utilisés en fonctionnement nominal. (voir T5-2.4) Les droits administrateurs devraient être associés au compte nominatif des utilisateurs en charge de la fonction d'administrateur technique.	*Catégorie de personnel*
5.2.1.4	Les comptes ayant des droits de type administrateur technique doivent être disjoints des comptes ayant des droits de type utilisateur métiers. Si une personne doit, selon les règles d'accès aux données telles que présentées dans l'exigence T5-1.1, bénéficier de profils de type administrateur technique et de profils de type utilisateur métier, elle doit avoir deux comptes utilisateur distincts, chacun nominatif et personnel. La multiplication des comptes nominatifs pour une même personne doit être restreinte au maximum. Aucune personne ne doit avoir plus de deux comptes nominatifs.	*Catégorie de personnel*
5.2.1.5	Chaque compte doit être associé à un dispositif d'authentification diffusé exclusivement et personnellement au titulaire du compte. En particulier, si le dispositif d'authentification n'intègre pas l'identité de l'utilisateur auquel il a été attribué (ex. calculette d'accès ou carte CPE), il convient, lors de sa diffusion, de rappeler à l'utilisateur que le dispositif est personnel et ne doit en aucun cas être laissé pour un usage « en libre-service ». La liste des comptes, de leur titulaire et du dispositif d'authentification associé devrait être élaborée et tenue à jour.	*Catégorie de personnel*
5.2.1.6	Afin de permettre une identification rapide de la finalité de chaque compte, il est recommandé que soit définie une nomenclature adaptée qui permette de distinguer les comptes d'utilisateur standard, les comptes d'administration (serveurs, postes de travail, équipements réseau, équipements sécurité), les comptes de service, les comptes utilisés par un équipement biomédical…	*Catégorie de personnel*

	Par exemple, on peut décider d'ajouter le suffixe « -ADMIN » à tout compte d'administrateur systèmes, « -RSX » à tout compte d'administration d'équipement réseau, « -SVC » à tout compte de service, « -MED » à tout compte attribué à un équipement biomédical, et de considérer que tout compte qui ne se termine pas par un de ces suffixes est un compte d'utilisateur standard.	

T5-2.2 Utiliser les dispositifs d'authentification en respectant les consignes de sécurité

Les dispositifs d'authentification utilisables sont les dispositifs identifiés dans les paliers de l'authentification privée du référentiel d'authentification des acteurs de santé de la PGSSI-S [Réf. n°6.12]. En substance il s'agit :

- identifiant/mot de passe ;
- dispositifs d'authentification à double facteurs diffusé par la structure ;
- cartes de la famille CPx (cartes CPS, CDE, CPE, CDA ou CPA) ou de solutions alternatives telles que décrites dans le référentiel d'authentification des acteurs de santé.

Exigence :

⇒ Les dispositifs utilisés pour s'authentifier sur le système d'information doivent être utilisés de manière à ne pas mettre en péril leur capacité à authentifier les personnes auxquelles ils ont été attribués.

Déclinaison en règles :

Règles sur l'utilisation des dispositifs d'authentification :

Réf.	Règles	Catégories de moyens du SI concernées
5.2.2.1	Les parties confidentielles des dispositifs d'authentification (mot de passe initial, code d'activation d'un dispositif d'authentification diffusé par la structure, code PIN d'une carte CPS, clé privée d'une bi-clé associée à un certificat électronique…) doivent être considérées comme des informations sensibles et traitées comme telles. Elles doivent être diffusées directement aux utilisateurs auxquels ces dispositifs ont été attribués de manière à en assurer la confidentialité (ex. enveloppe cachetée). Il est de la responsabilité de l'utilisateur du dispositif d'authentification de garder secret ces éléments.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels, Moyens d'authentification matériels (ex. carte CPS, « calculette de mot de passe unique »)*
5.2.2.2	En période d'utilisation, les dispositifs d'authentification doivent être maintenus sous le contrôle des utilisateurs auxquels ils ont été attribués. Hors période d'utilisation, s'ils ne peuvent pas rester sous le contrôle exclusif des utilisateurs auxquels ils ont été attribués, ils doivent être conservés dans un lieu sûr (pour éviter la perte et le vol).	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels, Moyens d'authentification matériels (ex. carte CPS, « calculette de mot de passe unique »)*

5.2.2.3	Dans le cas des cartes de la famille CPx, le code PUK doit être conservé en lieu sûr, soit par le porteur de la carte (en particulier pour des professionnels de santé pour des CPS comportant de multiples situations d'exercice notamment en dehors de la structure), soit par la structure (pour les cartes comportant exclusivement des situations d'exercice dans la structure).	*Moyens d'authentification matériels/carte CPx*
5.2.2.4	L'identification des utilisateurs du SI acteurs sanitaires et médico-sociaux doit se conformer au « Référentiel d'identification des acteurs sanitaires et médico-sociaux » de la PGSSI-S [Réf. n°6.11].	*Catégorie de personnel (ex. ensemble des utilisateurs et administrateurs du SI)*
5.2.2.5	L'authentification des utilisateurs du SI acteurs de santé doit se conformer au « Référentiel d'authentification des acteurs de santé » de la PGSSI-S [Réf. n°6.12].	*Catégorie de personnel*
5.2.2.6	Le choix des paliers pour l'identification des utilisateurs du SI acteurs sanitaires et médico-sociaux (cf. Réf. n°6.11) et pour l'authentification des utilisateurs du SI acteurs de santé (cf. Réf. n°6.12) devrait être réalisé en cohérence avec les enjeux liés à l'application web concernée.	*Catégorie de personnel*
5.2.2.7	Pour les utilisateurs du SI qui n'entrent pas dans le cadre des règles 5.2.2.4 à 5.2.2.6, s'ils ne bénéficient pas d'une identification nationale prévue pour être utilisée dans le cadre santé/médico-social, les éléments nécessaires à l'identification devraient être recueillis lors d'un processus enregistrement formalisé. L'identifiant attribué lors de cet enregistrement est alors un identifiant local délivré et géré sous la responsabilité de la structure.	*Catégorie de personnel*

T5-2.3 Protéger les comptes contre les tentatives d'usurpation d'identité

Exigence :

⇒ Les tentatives d'usurpation d'identité doivent être découragées sans pour autant impacter fortement les utilisateurs.

Déclinaison en règles :

Règles sur la protection des comptes :

Réf.	Règles	Catégories de moyens du SI concernées
5.2.3.1	Un verrouillage de compte pendant 1 minute minimum devrait être mis en place après trois essais de connexion infructueux.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.2.3.2	Les verrouillages de compte après trois essais de connexion infructueux devraient être tracés et conservés au même titre que les autres éléments de traçabilité mis en œuvre par le système d'information tels que décrits dans le thème 7-2.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.2.3.3	Le Référent Incident SSI devrait être alerté au bout de trois verrouillages de compte successifs dans la même journée. Il doit contacter le titulaire du compte pour vérifier que les tentatives ont bien été réalisées par celui-ci. Dans le cas contraire, la tentative d'usurpation du compte doit être considérée comme un incident de sécurité et gérée selon les modalités décrites dans le thème 7-3.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

T5-2.4 Protéger les comptes des services et les comptes administrateurs techniques par défaut

La création de comptes techniques attribués à certaines services ou applications qui s'exécutent dans un système est une pratique fortement recommandée, car elle permet une maîtrise accrue des droits attribués à ces services ou applications en les restreignant au strict minimum (par opposition à des services s'exécutant avec des droits « système »). La sécurité de ces comptes doit être gérée.
Les logiciels et les matériels intègrent souvent des comptes administrateurs techniques générique par défaut. Dans certains systèmes, il peut être impossible de les désactiver. L'une des caractéristiques de ce type de compte est de n'accepter que l'authentification par identifiant générique (ex. admin) et mot de passe. Même s'ils ne doivent pas être utilisés en fonctionnement nominal (cf. règle 5.2.1.3), ces comptes bénéficient de droits d'accès étendus. La protection des mots de passe de ces comptes doit donc être particulièrement encadrée.

Exigence :

⇒ Des mesures de protection des comptes administrateurs techniques par défaut doivent être mises en place pour s'assurer de leur non utilisation.

Déclinaison en règles :

Règles sur la protection des comptes administrateurs techniques par défaut :

Réf.	Règles	Catégories de moyens du SI concernées
5.2.4.1	Les mots de passe des comptes techniques de services (quand ils en requièrent un) et des comptes administrateurs techniques par défaut devraient être conservés dans un coffre numérique et sous enveloppe cachetée et stockés dans un endroit sûr (ex. coffre-fort, armoire fermant à clé…)	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.2.4.2	Si l'enveloppe contenant un mot de passe d'un compte administrateur technique par défaut est trouvée décachetée, le Référent Incident SSI devrait en être informé. Cette perte de confidentialité d'un mot de passe d'un compte administrateur technique par défaut doit être considérée comme un incident de sécurité et gérée selon les modalités décrites dans le thème 7-3.	*Catégories du personnel (ex. Responsable de la SSI, personnel du service informatique)*
5.2.4.3	Si, dans le cadre d'un accès exceptionnel, un utilisateur a dû utiliser un compte administrateur technique par défaut, le mot de passe de ce compte devrait être changé et la conservation du nouveau mot de passe doit respecter la règle 5.2.4.1.	*Catégories du personnel (ex. Responsable de la SSI, personnel du service informatique)*
5.2.4.4	Les dispositifs d'authentification (mots de passe des comptes ou certificats associés) par défaut devraient impérativement être modifiés au moment de l'installation de l'équipement ou de l'application, afin de garantir qu'aucun dispositif d'authentification ne reste tel qu'il a été défini par le constructeur ou l'éditeur.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.2.4.5	Les comptes de services et les comptes administrateurs techniques par défaut devraient être désactivés s'ils ne sont pas utilisés, conformément à la règle 4.5.3.11.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.2.4.6	Les droits attribués aux comptes de services et aux comptes administrateurs techniques par défaut devraient être réduit au strict minimum nécessaire à leur finalité.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.2.4.7	Si le service et le système le permettent, les comptes de services devraient être configurés pour interdire toute utilisation directe de ce compte par un utilisateur (i.e. : interdire l'usage de ces comptes pour l'authentification d'un utilisateur).	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

T5-3 Lutter contre les accès non autorisés

T5-3.1 Utiliser des moyens garantissant la sécurité des échanges

Exigence :

⇒ Il ne doit pas être possible d'accéder aux informations en dehors d'un accès authentifié.

Déclinaison en règles :

Règles sur le respect des bons usages en termes de comptes :

Réf.	Règles	Catégories de moyens du SI concernées
5.3.1.1	Tout accès à un logiciel ou un matériel contenant des informations sensibles et en particulier des données à caractère personnel doit se faire via une authentification sur un compte utilisateur mettant en œuvre des droits d'accès selon les règles énoncées dans les thèmes 5-1 et 5-2.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.3.1.2	Tout échange d'informations sensibles entre deux logiciels ou matériels doit de préférence se faire sur un réseau auquel l'accès est maitrisé selon les règles énoncées dans le thème 4-2.	*Equipements utilisateurs/Logiciels*
5.3.1.3	Si un échange d'information ne peut pas être réalisé sur un réseau maîtrisé, le flux d'échange devrait être protégé en confidentialité, soit par l'utilisation de logiciel sécurisé (ex. messagerie sécurisée), soit par le chiffrement du flux (ex. TLS).	*Equipements utilisateurs/Logiciels*
5.3.1.4	Quand des certificats sont mis en œuvre dans les applications ou équipements, les certificats et bi-clé fournis par défaut par le constructeur ou l'éditeur doivent impérativement être remplacés au moment de l'installation de l'équipement ou de l'application, afin de garantir qu'aucune bi-clé utilisée ne puisse rester connue d'un tiers. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir régénérer et modifier les bi-clés et certificats installés par défaut.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.3.1.5	L'utilisation de certificats électroniques, et plus généralement de moyens cryptographiques, devrait respecter les règles édictées par le RGS [Réf. n°9]. Cette règle est obligatoire pour les structures qui relèvent du secteur public.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
5.3.1.6	Les impressions d'informations sensibles devraient être effectuées selon une procédure prédéfinie, qui garantit le déclenchement de l'impression en présence de l'utilisateur concerné devant l'imprimante. Cette fonction, sur les systèmes d'impression qui la supportent, est typiquement réalisée par la mise en file d'attente de l'impression jusqu'à ce que l'utilisateur s'authentifie sur l'imprimante, à la suite de quoi l'impression effective est immédiatement déclenchée.	*Equipements utilisateurs/Terminaux /Imprimantes*

Thématique 6 : Acquérir des équipements, logiciels et services qui préservent la sécurité du SI

T6-1 Mettre en œuvre des prestations de télésurveillance, télémaintenance ou téléassistance

Les enjeux de SSI liés à la mise en œuvre de prestations de télésurveillance, télémaintenance ou téléassistance sont détaillés dans le guide pratique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé » [Réf. n°6.5] du corpus documentaire PGSSI-S. Ce document peut être utilement consulté pour plus d'informations sur le sujet.

Il est rappelé que le recours à un prestataire pour réaliser une activité ou fournir un service, n'exonère pas le responsable de la structure juridique de sa responsabilité (en particulier pénale). En sa qualité de responsable de traitement, le responsable du système d'information reste libre d'accepter ou non les clauses contractuelles etc…

T6-1.1 Encadrer la prestation par un contrat conforme aux règles du guide pratique « PGSSI-Règles d'intervention à distance »

Exigence :

⇒ Le guide pratique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé » [Réf. n°6.5] du corpus documentaire PGSSI-S constitue la base des règles applicables dans ce cadre. Le responsable du SI doit s'assurer que ceux de ses fournisseurs qui entrent dans le périmètre de ce guide en respectent les règles qui leur incombent.

Déclinaison en règles :

Règles sur l'encadrement de la prestation par un contrat conforme aux règles du guide pratique PGSSI-Règles d'intervention à distance :

Réf.	Règles	Catégories de moyens du SI concernées
6.1.1.1	Tout fournisseur réalisant des interventions à distance devrait s'engager par contrat au respect des règles du guide pratique PGSSI-Règles d'intervention à distance [Réf. n°6.5]. Il doit préciser le niveau de palier de règles qu'il atteint (palier intermédiaire : palier 1 ou palier supérieur : palier 2).	*Organisation (ex. Fournisseurs)*
6.1.1.2	Les documents contractuels principaux signés par les parties devraient être fournis en version papier au responsable du SI. Les autres documents, en particulier les annexes, peuvent être mis à disposition via internet sur l'espace client du site du fournisseur.	*Organisation*
6.1.1.3	Le fournisseur devrait établir un plan d'assurance sécurité qui décrit les dispositions de sécurité qu'il met en œuvre pour sa prestation (ou fait référence à une documentation de ces dispositions consultable par le responsable du SI).	*Organisation*

	Le plan d'assurance sécurité peut être un sous-ensemble du plan d'assurance qualité (PAQ). A la signature du contrat, le responsable du SI doit pouvoir indiquer s'il accepte le plan d'assurance sécurité type du fournisseur ou si un cycle de validation du plan d'assurance sécurité est nécessaire. Le plan d'assurance sécurité fait partie des documents applicables du contrat disponibles via internet sur l'espace client du site du fournisseur. Le plan d'assurance sécurité doit traiter au minimum les thèmes suivants : • critères de sécurité utilisés dans la désignation des personnes chargées de l'intervention à distance, engagement de sécurité, information de ces personnes sur la sécurité de la prestation et sensibilisation ; • règles de protection des informations relatives au SI ou à l'intervention et détenues par le fournisseur (copie, diffusion, conservation, destruction, transmission) ; • désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés, séparation vis-à-vis d'autres prestations ; • architecture générale de la plateforme utilisée pour l'intervention à distance, cloisonnement technique vis-à-vis d'autres prestations, fonctions de sécurité activées dans la plateforme ; • accès logique des intervenants à la plateforme, identification et authentification, mise en veille et déconnexion automatiques, séparation des tâches, gestion des droits, traçabilité des actions ; • dispositions prises pour continuer à assurer les activités de la prestation à la suite d'un incident majeur ; • assurance et contrôle de la sécurité des services d'intervention fournis.	
6.1.1.4	Le fournisseur et le responsable du SI devraient définir les modalités pratiques permettant la bonne réalisation de l'intervention à distance (convention de service). Les modalités pratiques doivent être portées à la connaissance des personnes concernées. Elles doivent préciser la prestation : • objectifs et périmètre des interventions à distances prévues ; • obligations réciproques du fournisseur et du responsable du SI ; • moyens mis en œuvre ; • procédures, ou référence aux documents de procédures ; • règles de sécurité particulières.	*Organisation*
6.1.1.5	A ce titre, les dispositions organisationnelles de sécurité suivantes devraient au minimum être prises en compte :	*Organisation*

	• toute intervention de télémaintenance doit faire l'objet d'un rapport transmis à son bénéficiaire par le fournisseur, dans les meilleurs délais ;
	• les interventions de téléassistance s'effectuent sous le contrôle de leur bénéficiaire. Il appartient à chaque bénéficiaire :
	  ○ d'autoriser explicitement la prise de main ou le suivi à distance de son poste de travail (affichage d'une demande d'action d'autorisation sur le poste par exemple),
	  ○ d'exiger, s'il le souhaite, de moduler l'accès aux données ;
	• tout bénéficiaire doit avoir la possibilité technique d'interrompre à tout moment la téléassistance en cours et doit avoir été formé sur la mise en œuvre de cette fonctionnalité.	

T6-1.2 Mettre en œuvre des dispositions techniques de sécurité spécifiques dans le SI

Exigence :

⇒ Les SI doit être protégé des menaces liées à l'ouverture d'accès permettant l'intervention à distance.

Déclinaison en règles :

Règles sur des dispositions techniques de sécurité spécifiques aux accès d'intervention à distance :

Réf.	Règles	Catégories de moyens du SI concernées
6.1.2.1	Dans la mesure du possible, l'accès aux équipements objets de l'intervention à distance doit être réalisé à travers un point d'accès distant (ou passerelle) mis en place à cet effet. Dans ce cas : • si les équipements concernés n'ont pas besoin de communiquer avec le reste du SI, ou s'ils disposent d'une interface réseau dédiée à l'administration, ou encore s'ils peuvent être rattachés à plusieurs VPN, ils doivent être reliés à ce point d'accès de préférence par un réseau d'administration dédié (réseau physique séparé ou VPN) ; • le point d'accès distant doit être protégé contre les attaques logiques en provenance des réseaux externes (fournisseur, Internet,…) et son contournement en vue d'accéder au réseau du SI ne doit pas être possible dans la pratique ; • Le point d'accès distant ne doit autoriser les communications internes au SI qu'avec les équipements prévus et les équipements permettant l'administration du point d'accès lui-même.	*Equipements d'infrastructure* *système et réseau* *Equipements utilisateurs*

6.1.2.2	Si la mise en œuvre d'un point d'accès distant n'est pas possible, la connexion directe du télé-mainteneur sur des équipements contenant des applications ou des informations à caractère personnel peut être envisagée. Il appartient alors au responsable du SI de décider, sur recommandation du fournisseur, de la solution et du protocole utilisés pour l'échange entre les équipements objets de l'intervention et la plateforme. Dans ce cas: • les échanges doivent être protégés de bout en bout par des fonctions de chiffrement et d'authentification mutuelle ; ces fonctions doivent être de préférence conformes au Référentiel Général de Sécurité[12] ; • un dispositif de filtrage doit autoriser uniquement les flux nécessaires à l'intervention à distance. Ce dispositif peut être à base de filtrage d'adresse IP ou de liste blanche de certificat par exemple.	*Equipements d'infrastructure* *système et réseau* *Equipements utilisateurs*
6.1.2.3	Chaque équipement objet d'une télésurveillance ou d'une télémaintenance doit disposer d'un compte réservé à cet usage et dont les paramètres d'identification et d'authentification sont spécifiques à l'équipement (i.e. différents de ceux utilisés pour tout autre équipement).	*Equipements d'infrastructure* *système et réseau* *Equipements utilisateurs*
6.1.2.4	Le responsable du SI (ou le Responsable de la SSI) doit disposer d'un espace de stockage dans lequel les traces des accès et des opérations effectuées à distance sont centralisées et conservées sous son contrôle, en vue d'être exploitées à des fins de vérification et en cas de litige ou d'incident.	*Equipements d'infrastructure* *système et réseau* *Equipements utilisateurs*

[12] Voir annexe du RGS [Réf. n°9] consacrée à la confidentialité - http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html

T6-2 Acquérir des dispositifs connectés

Les enjeux de SSI liés à l'acquisition et la mise en œuvre de dispositifs connectés sont détaillés dans le guide pratique « Règles pour les dispositifs connectés d'un Système d'Information de Santé» [Réf. n°6.6] du corpus documentaire PGSSI-S. Ce document peut être utilement consulté pour plus d'informations sur le sujet.

T6-2.1 Demander aux industriels et fournisseurs un engagement de conformité au guide pratique « PGSSI-Dispositifs connectés »

Exigence :

⇒ Le guide pratique «Règles pour les dispositifs connectés d'un Système d'Information de Santé» [Réf. n°6.6] du corpus documentaire PGSSI-S constitue la base des règles applicables aux dispositifs connectés. Le responsable du SI doit s'assurer que ceux de ses fournisseurs qui entrent dans le périmètre de ce guide en respectent les règles qui leur incombent.

Déclinaison en règles :

Règles sur la conformité des dispositifs connectés aux règles du guide pratique PGSSI-Dispositifs connectés :

Réf.	Règles	Catégories de moyens du SI concernées
6.2.1.1	Tout fournisseur d'un équipement connecté, quel que soit le cadre de l'obtention de l'équipement par la structure (prêt, location, achat, expérimentation ou développement en collaboration, etc.), devrait s'engager sur la conformité de ses pratiques et du dispositif fourni à chacune des règles du guide [Réf. n°6.6]. Il doit également indiquer le niveau de palier globalement atteint (palier intermédiaire : palier 1 ou palier supérieur : palier 2).	*Equipements utilisateurs (ex. Equipements biomédicaux connectés au SI)*

T6-2.2 Obtenir un accès aux documentations requises par le guide pratique « PGSSI-Dispositifs connectés »

Exigence :

⇒ Afin que les implications en termes de SSI de l'utilisation du dispositif connecté puissent être pleinement prises en compte, les documentations prévues par le guide pratique «Règles pour les dispositifs connectés d'un Système d'Information de Santé» [Réf. n°6.6] du corpus documentaire PGSSI-S doivent être accessibles au responsable du SI de la structure.

Déclinaison en règles :

Règles sur l'accès aux documentations requises par le guide pratique PGSSI-Dispositifs connectés:

Réf.	Règles	Catégories de moyens du SI concernées
6.2.2.1	Le fournisseur et/ou le fabricant devrait identifier dans la documentation, fournie ou accessible à la structure (par exemple au travers d'un espace client sur Internet), l'ensemble des composants matériels (serveurs, périphériques, …) et logiciels (versions des logiciels, systèmes d'exploitation, bases de données, …) informatiques standards constituant le dispositif connecté ainsi que leurs principales caractéristiques.	*Equipements utilisateurs*
6.2.2.2	Le fournisseur et/ou le fabricant devrait identifier, dans la documentation qu'il met à disposition, l'ensemble des spécifications portant sur le poste d'administration/utilisation du dispositif connecté (caractéristiques matérielles du poste, version du système d'exploitation, middleware et pilotes, services activés, périphériques, …).	*Equipements utilisateurs*
6.2.2.3	Le fournisseur et/ou le fabricant devrait identifier, dans la documentation qu'il met à disposition, l'ensemble des mesures de sécurité physique (sécurité des locaux, clés du coffret protégeant le dispositif connecté, contraintes d'environnement notamment compatibilité électromagnétique (réseau Wifi, téléphone mobile), sécurité des câblages…) préconisées pour la mise en œuvre du dispositif connecté au sein du SI.	*Equipements utilisateurs*
6.2.2.4	Le fournisseur et/ou le fabricant devrait indiquer, dans la documentation qu'il met à disposition, la méthode d'analyse de risques qu'il a appliquée pour l'analyse de risques de son équipement, les risques couverts par les mesures qu'il a mises en application et les risques résiduels portés par le client (si il les accepte).	*Equipements utilisateurs*

T6-2.3 Identifier les solutions de réversibilité permettant une reprise des données

Exigence :

⇒ Les données conservées par un équipement connecté doivent pouvoir être récupérées par la structure, si elle le souhaite, pour les réutiliser dans un dispositif différent quand elle décide de ne plus mettre en œuvre le dispositif connecté.

Déclinaison en règles :

Règles sur la nécessité de solutions de réversibilité permettant une reprise des données d'un dispositif connecté :

Réf.	Règles	Catégories de moyens du SI concernées
6.2.3.1	Le fournisseur et/ou le fabricant devrait proposer des solutions de réversibilité permettant une reprise des données dans un format réutilisable par le client, notamment en cas de changement d'équipement.	*Equipements utilisateurs*

T6-3 Acquérir des progiciels « sur étagère »

T6-3.1 Demander aux industriels et fournisseurs un engagement de conformité au guide pratique « Accès Tiers » en cas d'applicabilité

Le guide pratique « Règles pour la mise en place d'un accès web au SIS pour des tiers »» [Réf. n°6.6] du corpus documentaire PGSSI-S fixe un ensemble de règles qui concernent la mise en œuvre d'interfaces destinées à permettre l'accès de tiers à des services en ligne fournis par un SI. Le respect de ces règles, ou des règles équivalentes pour l'environnement de développement concerné, doit être attendu de la part des industriels et fournisseurs de progiciels « sur étagère » pour les développements de logiciels qu'ils réalisent.

Ce document peut être utilement consulté pour plus d'informations sur le sujet.

Exigence :

⇒ Les industriels et fournisseurs de progiciels « sur étagère » doivent respecter les règles de bonnes pratiques référencées par le guide pratique « Règles pour la mise en place d'un accès web au SI pour des tiers » [Réf. n°6.7] du corpus documentaire PGSSI-S, ou des règles équivalentes dans l'environnement de développement qu'ils utilisent.

⇒ Les changements apportés par le GHT SLS aux progiciels sont interdits. Les changements doivent être demandés à l'éditeur directement.

Déclinaison en règles :

Règles sur l'engagement de conformité au guide pratique « Accès Tiers » en cas d'applicabilité :

Réf.	Règles	Catégories de moyens du SI concernées
6.3.1.1	Les industriels et fournisseurs de progiciels « sur étagère » devraient s'engager formellement à respecter les bonnes pratiques de développement logiciel, et notamment en ce qui concerne la sécurité : • si les progiciels qu'ils proposent sont de type « application ou service web », ils devraient s'engager à respecter le guide pratique « Règles pour la mise en place d'un accès web au SI pour des tiers » [Réf. n°6.7] du corpus documentaire PGSSI-S et en particulier les bonnes pratiques en matière de développement publiées par l'OWASP et l'ANSSI. • dans les autres cas, ils devraient communiquer les référentiels de bonne pratique qu'ils appliquent en matière de prise en compte de la SSI dans leurs développements.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

T6-3.2 Vérifier les fonctionnalités de sécurité au regard de la PSSI

Exigence :

⇒ Les progiciels « sur étagère » acquis par la structure doivent intégrer les fonctions de sécurité qui permettent leur mise en œuvre conformément aux règles énoncées par la PSSI de la structure.

Déclinaison en règles :

Règles sur la vérification des fonctionnalités de sécurité :

Réf.	Règles	Catégories de moyens du SI concernées
6.3.2.1	Si le progiciel propose une méthode d'authentification des utilisateurs par mot de passe, il convient de vérifier, préalablement à son acquisition : • que cette méthode est suffisante au regard des référentiels d'authentification du corpus documentaire PGSSI-S [Réf. n°6] ; • que le progiciel propose l'ensemble des fonctions de gestion des mots de passe répondant aux règles de la thématique 4-5.1 (longueur des mots de passe, renouvellement, …).	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
6.3.2.2	Il convient de vérifier, préalablement à l'acquisition du progiciel, qu'il intègre les fonctions de gestion des accès aux informations conforme aux règles de la thématique 5-1 (gestion de rôles, fonctions d'affectation/retrait/contrôle des droits, comptes administrateurs, …)	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*

T6-4 Acquérir des équipements informatiques

T6-4.1 Demander aux industriels et fournisseurs un engagement de conformité au guide pratique « Destruction de données lors de transfert de matériels informatiques »

Les règles ci-dessous sont principalement issues du guide pratique « Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé » [Réf. n°6.9] du corpus documentaire PGSSI-S.

Ce document peut être utilement consulté pour plus d'informations sur le sujet.

Exigence :

⇒ Les industriels et fournisseurs susceptibles d'être destinataires d'équipements contenant des données retournées par la structure (par exemple dans le cadre d'un contrat de maintenance, de garantie du matériel, de location ou de prêt) doivent s'engager à mettre en œuvre les modalités de destruction des données requises par le PSSI.

Déclinaison en règles :

Règles sur l'engagement des fournisseurs en matière de destruction des données :

Réf.	Règles	Catégories de moyens du SI concernées
6.4.1.1	Les industriels et fournisseurs susceptibles d'être destinataires de supports de données (par exemple dans le cadre d'un contrat de maintenance, de garantie du matériel, de location ou de prêt) devraient s'engager à mettre en œuvre les modalités de destruction des données énoncées à la thématique 3-1.4 de la PSSI. Ces règles peuvent également être consultées via le Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé [Réf. n°6.9].	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.4.1.2	Les fournisseurs devraient mettre à disposition de la structure les procédures : • d'effacement des données ; • de réinitialisation en configuration d'usine. pour ces terminaux.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.4.1.3	Les clauses générales suivantes devraient figurer aux contrats : • le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative ; • le fournisseur doit soumettre toute sous-traitance de prestation à l'autorisation du responsable du SI ; • en cas de recours à la sous-traitance, le fournisseur doit répercuter les exigences qui lui sont applicables vers le sous-traitant.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.4.1.4	Les clauses de sécurité suivantes devraient figurer aux contrats :	*Equipements d'infrastructure système et réseau,*

	• le fournisseur doit s'engager vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée doit avoir signé un engagement individuel de confidentialité rappelant les dispositions de la loi Informatique & Libertés et les sanctions applicables ; • le responsable du SI a la possibilité de faire réaliser des audits de sécurité des dispositions prises par le fournisseur pour la réalisation de sa prestation.	*Equipements utilisateurs*
6.4.1.5	Les exigences de sécurité suivantes devraient figurer au contrat : • le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la confidentialité des données lors de transferts de matériel.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.4.1.6	Les équipements fournis devraient présenter des caractéristiques compatibles avec les règles de la PSSI. Par exemple, la structure, ou à défaut le fournisseur, devrait : • avoir la capacité d'effacement des supports de stockage de dispositifs connectés ; • pouvoir remettre en configuration d'usine les matériels de type « ordiphone », avec effacement de l'ensemble des données.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T6-5 Encadrer les développements spécifiques et les acquisitions de logiciels, d'équipements du SI, d'équipements connectés et de services liés au SI

T6-5.1 Intégrer la SSI dans les cahiers des charges

Exigence :

⇒ Les modifications apportées au SI, qu'il s'agisse d'ajout de nouveaux composant ou de modification des composants ou de l'architecture existante, que leur origine soit une acquisition, une location, une mise à disposition, un développement interne ou externe, doivent faire l'objet d'une spécification précise qui intègre la dimension SSI et être soumises à validation avant d'être engagées.

Déclinaison en règles :

Règles sur l'intégration de la SSI dans les cahiers des charges :

Réf.	Règles	Catégories de moyens du SI concernées
6.5.1.1	Toute modification technique ou applicative du SI devrait faire l'objet d'une spécification formalisée dans un cahier des charges, qui prenne en compte les aspects SSI liés au périmètre concerné du SI, sans omettre les points relatifs à la sauvegarde des données et à la continuité de fonctionnement.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.2	Si la modification technique ou applicative du SI envisagée change le périmètre technique (ex : nouveau type d'équipement, télémaintenance, externalisation) ou fonctionnel (ex : nouvelle application) du SI, ou introduit de nouveaux acteurs (ex : changement de prestataire d'hébergement externe des sauvegardes), une analyse de risque devrait être menée afin d'identifier les nouveaux risques éventuellement introduits et de vérifier qu'ils sont acceptables pour les responsables des SI concernés.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.3	Les modifications techniques et applicatives du SI doivent éviter autant que possible toute adaptation spécifique de composants sur étagère (logiciels notamment).	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.4	En cas de remplacement d'une application qui traite des données d'usagers, l'opération devrait prévoir la migration des données existantes afin de respecter les exigences quant à la durée de conservation de ces données. A défaut, l'ancienne application devrait être conservée pour permettre au moins l'accès aux données existantes.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.5	Les modifications ou mises en place d'accès web par des tiers au SI devraient se conformer aux règles énoncées par le guide pratique « Règles pour la mise en place d'un accès web au SI pour des tiers » [Réf. n°6.7] du corpus documentaire PGSSI-S. Il est recommandé que ces règles soient également intégrées aux cahiers de charges des projets de nature différente dès lors qu'elles sont applicables ou qu'elles peuvent être adaptées au contexte technique du projet.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

6.5.1.6	Le cahier des charges devrait être soumis à l'approbation du responsable du SI concerné et du Responsable de la SSI avant tout démarrage des travaux.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.7	La structure peut prévoir une procédure de changement en urgence, qui, sur autorisation du comité de production du SI concerné (voir 2.1.1.11) pour des circonstances exceptionnelles, permet une réalisation de modifications du SI, le cas échéant directement en production, documentée a posteriori. La procédure devrait prévoir l'information de l'autorité d'homologation du SI sur les risques induits par la modification mis en regard des enjeux justifiant la procédure d'urgence. Le Responsable de la SSI doit être consulté sur le sujet.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.8	Les principes et fonctions de sécurité nécessaires aux développements réalisés ou aux produits ou services acquis devraient se conformer au Référentiel Général de Sécurité [Réf. n°9]. Cette règle est obligatoire pour les structures qui relèvent du secteur public.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.1.9	Lorsqu'ils sont disponibles pour répondre aux fonctions de sécurité nécessaires aux développements réalisés ou aux produits ou services acquis, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés. Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/administration/qualifications/ http://www.ssi.gouv.fr/administration/produits-certifies/ Cette règle est obligatoire pour les structures qui relèvent du secteur public.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T6-5.2 Valider les nouveaux composants du SI avant leur mise en production

Exigences :

⇒ Les modifications apportées au SI doivent faire l'objet d'une procédure de recette avant leur mise en production effective.

⇒ Tout compostant technique du système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies.

Déclinaison en règles :

Règles sur la validation des composants du SI avant leur mise en production :

Réf.	Règles	Catégories de moyens du SI concernées
6.5.2.1	Toute modification technique ou applicative du SI (y compris évolution de version) devrait faire, préalablement à toute mise en production, l'objet d'un processus de recette, formalisé par une procédure établie par la structure, qui vérifie la conformité des composants concernés au cahier des charges tant du point de vue du SI que de celui des utilisateurs. Les modalités de sauvegarde de configurations et de données, ainsi que celle liées à la continuité de fonctionnement des composants concernés devraient être documentées et testées avant mise en production.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.2.2	Si les composants concernés participent à l'accès web par des tiers au SI, des tests spécifiques (notamment des tests de vulnérabilité et d'intrusion) devraient être menés, comme spécifié dans le guide pratique « Règles pour la mise en place d'un accès web au SI pour des tiers » [Réf. n°6.7] du corpus documentaire PGSSI-S.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.2.3	Il est recommandé de procéder, au cours de la recette, à un test de vulnérabilité des composants concernés une fois intégrés au SI (environnement de test), afin de détecter les éventuelles failles connues et de les corriger avant la mise en production.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.2.4	Le processus de recette devrait être réalisé dans un environnement dédié aux tests, distinct de l'environnement de production.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.2.5	Les données utilisées pour les tests ne devraient en aucun cas comporter de données nominatives réelles.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.2.6	Seuls les composants techniques (équipements, applications, liaisons réseau…) homologués par Commission habilitation et sécurité (voir 2.1.1.11) devraient être mis en production, qu'il s'agisse de composants nouveaux ou de composants modifiés.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
6.5.2.7	La décision d'homologation d'un composant technique du SI est prononcée par Commission habilitation et sécurité sur la base (liste non limitative) :	*Equipements d'infrastructure système et réseau,*

	• des éléments prévus au cahier des charges ; • de l'analyse de risques réalisée le cas échéant ; • du rapport de recette du composant ; • de la disponibilité de la documentation relative au composant, constituée des éléments requis par la règle 4.1.5.1, et qui doit être intégrée ou mise à jour dans le référentiel de documentation du SI conformément à la règle 4.1.5.3.	*Equipements utilisateurs*
6.5.2.8	En cas de mise en œuvre de la procédure de changement en urgence, des mesures de contrôle du bon fonctionnement des modifications effectuées et de l'absence d'effet de bord devraient être prévues et appliquées. L'autorité d'homologation du SI doit être informée des conclusions de ces contrôles et la documentation des changements effectués doit lui être communiquée.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T6-5.3 Assurer la formation aux nouveaux composants du SI

Exigence :

⇒ Les personnes en charge de l'exploitation du SI et les utilisateurs du SI doivent être formées aux nouveaux composants du SI ou aux changements qui leur sont apportés.

Déclinaison en règles :

Règles sur la formation aux composants du SI :

Réf.	Règles	Catégories de moyens du SI concernées
6.5.3.1	Les personnels en charge de l'administration et de l'exploitation des infrastructures et des applications du SI devraient être formés à la réalisation des tâches qui leur incombent, pour chacun des composants nouveaux ou modifiés, conformément aux règles 2.2.1.3 et 2.2.1.5.	*Catégorie de personnel (ex. Personnel du service informatique)*
6.5.3.2	Les utilisateurs du SI devraient être formés à l'utilisation des applications et équipements nouveaux ou modifiés du SI qui leur sont destinés, conformément aux règles 2.2.1.4 et 2.2.1.5.	*Catégorie de personnel (ex. tout utilisateur du SI)*

T6-6 Définir l'objet des prestations et les limites d'engagement dans les relations contractuelles avec les tiers fournisseurs de service

T6-6.1 Définir précisément dans le contrat le contenu des prestations confiées au tiers fournisseur de service pour répondre aux obligations de sécurité

☞ Le contrat permet, par la description du contenu des prestations confiées au tiers fournisseur de service par le responsable de la structure, de préciser la répartition des responsabilités entre le fournisseur de service et la structure.

La structure et son représentant (ou délégataire) responsable du traitement de données à caractère personnel ***restent libres d'accepter ou non les clauses contractuelles proposées*** par le prestataire. Il leur appartient de ***veiller à ne pas accepter de clauses et conditions contractuelles, ni l'absence de clauses nécessaires, qui seraient contraires à la législation sur la protection des données***.

Exigence :

⇒ Les contrats établis avec des tiers fournisseurs de services doivent intégrer les clauses permettant le respect des exigences de sécurité auxquelles est soumise la structure, et des règles énoncées par la PSSI.

Déclinaison en règles :

Règles sur la contractualisation avec les tiers fournisseurs de service :

Réf.	Règles	Catégories de moyens du SI concernées
6.6.1.1	Le contrat d'externalisation devrait contenir à minima les clauses listées à l'article R 1111-13 du code de la santé publique.	*Organisation (ex. Fournisseurs)*
6.6.1.2	Le contrat devrait présenter les caractéristiques suivantes : • l'objet du contrat doit être précis ; • les rôles et responsabilités des parties doivent être clairement définis ; • le fournisseur est tenu d'effectuer toutes les activités liées aux données à caractère personnel et en particulier de santé au sein de l'Union Européenne ou conformément aux règles définies par la CNIL pour les interventions hors Union Européenne[13] ; • le fournisseur garantit la disponibilité, l'intégrité, la confidentialité, l'auditabilité, la pérennité des données. Ce qui se traduira par des mesures techniques et d'organisation interne ; • le fournisseur doit s'engager vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée doit avoir été sensibilisée à la confidentialité des données et avoir signé un engagement individuel de confidentialité rappelant	*Organisation*

[13] http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/

	les dispositions de la loi Informatique & Libertés et les sanctions applicables ; • le fournisseur doit s'engager vis-à-vis des actions que le personnel peut effectuer. Chaque personne concernée doit avoir signé un engagement individuel de limitation de ses actions au seul besoin des interventions ; • le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative ; • le fournisseur doit soumettre toute sous-traitance de prestation à l'autorisation du responsable du SI ; • en cas de recours à la sous-traitance, le fournisseur doit répercuter les exigences qui lui sont applicables vers le sous-traitant ; • des mesures de contrôle et d'audit réalisées par le responsable du SI peuvent être prévues dans le contrat.	
6.6.1.3	Le contrat devrait prévoir que le tiers fournisseur de service s'engage à respecter les règles de la PSSI et les référentiels cités en référence qui le concernent.	*Organisation*

T6-6.2 S'assurer de la capacité de restitution des données de santé à caractère personnel, et plus généralement de toute donnée confiée, sous une forme réutilisable par la structure

Exigences :

⇒ Tout recours à une prestation qui inclut un hébergement de données, et en particulier de données de santé à caractère personnel, doit prévoir les modalités :

- de restitution de ces données au responsable du traitement à l'issue de cet hébergement ;
- de l'effacement de ces données de l'environnement de l'hébergeur.

⇒ En particulier, le contrat de prestation doit engager le prestataire, sans autre condition que la fin de sa prestation d'hébergement de données et quelle qu'en soit la cause, sur :

- la restitution de l'intégralité des données confiées (données de santé à caractère personnel ou autres) ;
- les modalités pratiques de restitution de ces données : format, sécurisation des données et de leur transfert, support d'échange. Ces modalités doivent permettre à la structure de poursuivre son activité ou de recourir à un autre prestataire pour l'hébergement des données ;
- la fourniture de l'ensemble des documentations et programmes éventuellement nécessaires à l'exploitation des données restituées ;
- l'effacement de toute copie et sauvegarde des données qui lui ont été confiées. Cet effacement doit être réalisé en conformité avec les règles du Guide de destruction des données [Réf. n°6.9] ;
- la fourniture de l'assistance nécessaire durant la période de migration pour faciliter d'une part le transfert des données et des moyens de sécurisation associés et d'autre part la reprise de leur exploitation par la structure ou par toute autre organisation qu'elle aura désignée.

Déclinaison en règles :

Règles sur la restitution et l'effacement des données qui ont été confiées à un prestataire :

Réf.	Règles	Catégories de moyens du SI concernées
6.6.2.1	Tout contrat de prestation qui inclut un hébergement de données, et en particulier un hébergement de données de santé à caractère personnel, devrait engager le prestataire sur les modalités de restitution et d'effacement des données qui lui ont été confiées, à la fin de sa prestation d'hébergement de données sans autre condition et quelle qu'en soit la cause.	*Organisation (ex. Prestataire d'hébergement de données)*
6.6.2.2	Le prestataire devrait s'engager à restituer, à l'issue de sa prestation d'hébergement de données, l'intégralité des données qui lui ont été confiées.	*Organisation*
6.6.2.3	Le prestataire devrait s'engager à restituer les données qui lui ont été confiées dans le format spécifié en annexe	*Organisation*

	du contrat (ex. format XML), support, scellement, chiffrement, transfert physique.	
6.6.2.4	Le prestataire devrait s'engager à fournir l'ensemble des documentations et programmes éventuels nécessaires à l'exploitation des données restituées.	*Organisation*
6.6.2.5	A réception des données restituées par le prestataire, le responsable du traitement fait procéder à la vérification de l'intégrité des données et à leur intégration dans le système de stockage cible. Il fait confirmer que l'ensemble des données attendues ont été intégrées et qu'elles sont exploitables. Dès lors qu'il est vérifié que les données ont été sauvegardées avec succès selon la politique de sauvegarde du système cible, le responsable du traitement notifie le prestataire de la bonne intégration des données et lui demande de procéder à l'effacement définitif des données qu'il détient.	*Organisation*
6.6.2.6	Le prestataire devrait s'engager à procéder à l'effacement de tout enregistrement, copie ou sauvegarde des données restituées, quand le responsable du traitement le lui demande à l'issue de la prestation qu'il fournit. Cet effacement doit être réalisé en conformité avec les règles de destruction des données. (cf. règles de la thématique 3-1.4)	*Organisation*
6.6.2.7	Le prestataire devrait s'engager à fournir l'assistance nécessaire durant la période de migration des données afin de faciliter leur transfert ainsi que la reprise de leur exploitation par la structure ou par toute autre organisation qu'elle aura désignée.	*Organisation*

T6-6.3 Clauses de sécurité en cas d'externalisation de la destruction des données

Les règles ci-dessous sont issues du guide pratique « Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé » [Réf. n°6.9] du corpus documentaire PGSSI-S.

Ce document peut être utilement consulté pour plus d'informations sur le sujet.

Exigence :

⇒ Quand il est envisagé d'avoir recours à un prestataire de service pour la destruction de données, les exigences de sécurité formulées par la PSSI sur ce sujet doivent être intégrées au contrat d'externalisation.

Déclinaison en règles :

Règles relatives aux contrats d'externalisation de la destruction des données :

Réf.	Règles	Catégories de moyens du SI concernées

6.6.3.1	Les clauses générales suivantes devraient figurer au contrat : • le fournisseur est tenu d'effectuer toutes les activités liées à ce type d'intervention au sein de l'Union Européenne ou conformément aux règles définies par la CNIL pour les interventions réalisées hors Union Européenne; • le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative ; • le fournisseur doit soumettre toute sous-traitance de prestation à l'autorisation du responsable du SI ; • en cas de recours à la sous-traitance, le fournisseur doit répercuter les exigences qui lui sont applicables vers le sous-traitant.	*Organisation (ex. Prestataire de destruction des supports de données)*
6.6.3.2	Les clauses de sécurité suivantes devraient figurer au contrat : • le fournisseur doit s'engager vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée doit avoir signé un engagement individuel de confidentialité rappelant les dispositions de la loi Informatique & Libertés et les sanctions applicables ; • le responsable du SI a la possibilité de faire réaliser des audits de sécurité des dispositions prises par le fournisseur pour la réalisation de sa prestation.	*Organisation*
6.6.3.3	L'exigence de sécurité suivante devrait figurer au contrat : • le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la confidentialité des données lors de transferts de matériel.	*Organisation*

Thématique 7 : Limiter la survenue et les conséquences d'incidents de sécurité du SI

T7-1 Vérifier le niveau de sécurité des moyens informatiques

T7-1.1 Procéder à un contrôle régulier de la bonne mise en œuvre des règles de la PSSI

Exigence :

⇒ Le Responsable de la SSI doit réaliser ou faire réaliser un contrôle régulier de la mise en œuvre effective des règles de sécurité prévues par la PSSI.

Déclinaison en règles :

Règles sur le contrôle de la mise en œuvre des règles de la PSSI :

Réf.	Règles	Catégories de moyens du SI concernées
7.1.1.1	Le Référent SSI devrait vérifier régulièrement la mise en œuvre effective des règles de sécurité qui doivent être appliquées conformément aux objectifs fixés par les Plans d'Action SSI successifs, ceci doit être fait dans le cadre du SMSI. Il peut pour cela : • demander aux responsables en charge de parties du SI d'effectuer une auto-évaluation ; • procéder à ce contrôle lui-même ; • mandater un prestataire externe pour cette tâche. Un bilan annuel de l'ensemble du périmètre des règles applicables est recommandé.	*Catégorie de personnel (ex. Responsable de la SSI)*
7.1.1.2	Si la conformité de mise en œuvre des règles est effectuée par auto-évaluation par les personnes en charge de l'application des règles, le périmètre complet devrait être également contrôlé par le Responsable de la SSI ou par une personne externe mandatée par lui, mais sur une période plus longue. Un contrôle complet par le Responsable de la SSI sur une période de 3 ans est recommandé (par exemple, par contrôle d'un tiers du périmètre chaque année).	*Catégorie de personnel*
7.1.1.3	Quand les contrôles sont réalisés sur un échantillon de règles, les règles sur lesquelles se concentre chaque campagne de contrôle devraient être choisies en fonction : • du délai écoulé depuis leur mise en œuvre ou leur dernière vérification ; • de leur priorité de mise en œuvre ; • d'éventuels incidents qui pourraient indiquer un défaut dans leur application.	*Catégorie de personnel*

7.1.1.4	Pour chaque règle, le contrôle devrait prendre en compte les aspects suivants : • l'intégration des éléments de la règle dans les procédures documentées du domaine concerné ; • le cas échéant, le résultat effectif de l'application de la règle (ex. analyse des contrats de télémaintenance pour les règles des thèmes T6-1 et T6-6, présence effective et efficacité du cloisonnement réseau pour les règles du thème T4-2…).	*Catégorie de personnel*
7.1.1.5	La vérification ne devrait pas omettre les parties externalisées du SI. Les prestataires devraient fournir une attestation de bonne mise en œuvre des règles qui leur incombent (équivalent de l'auto-évaluation) et, dans le cadre du contrôle effectué par le Responsable de la SSI, soit permettre une vérification par le Responsable de la SSI lui-même, soit faire réaliser le contrôle par un tiers, selon les modalités prévues par le contrat d'externalisation.	*Catégorie de personnel*
7.1.1.6	Le Responsable de la SSI devrait procéder (ou faire procéder) à une vérification au moins annuelle de la conformité des règles de cloisonnement et des ouvertures de flux effectivement mises en œuvre suite aux principes fixés par les règles de la PSSI et aux besoins identifiés pour les différents flux légitimes recensés, comme définis en T4-2.2 et en T4-3.2.	*Catégorie de personnel*
7.1.1.7	La revue des droits d'accès mis en œuvre selon les principes énoncés dans le thème T5-1.3 devrait être intégrée au programme de revue avec une périodicité au moins annuelle.	*Catégorie de personnel*
7.1.1.8	Le Responsable de la SSI devrait vérifier que les dispositifs qui fournissent des services techniques nécessaires au bon fonctionnement et à la sécurité du SI (voir 3eme liste dans la règle 3.1.1.1, notamment système de lutte anti-incendie, climatisation, système anti-intrusion) sont testés régulièrement. Cette vérification sur la base de compte-rendu de test établi, quand c'est applicable, par un organisme certifié et disposant des agréments nécessaires. Le Responsable de la SSI devrait s'assurer que les éventuels dysfonctionnements détectés sont rapidement corrigés. Si nécessaire, il devrait procéder (ou faire procéder) à ces vérifications.	*Catégorie de personnel*
7.1.1.9	La revue de la documentation du SI et de ses modalités de stockage et de protection en conformité avec les principes énoncés dans le thème T4-1.5 devrait être intégrée au programme de revue avec une périodicité au moins annuelle.	*Catégorie de personnel*

T7-1.2 Procéder à un audit régulier des vulnérabilités du SI

Exigence :

⇒ Le Responsable de la SSI doit faire réaliser régulièrement un audit des vulnérabilités du SI.

Déclinaison en règles :

Règles sur l'audit des vulnérabilités du SI :

Réf.	Règles	Catégories de moyens du SI concernées
7.1.2.1	Le Responsable de la SSI doit faire réaliser régulièrement un audit des vulnérabilités du SI sur les aspects : • techniques : architecture, systèmes, applications, réseaux dont réseaux sans fils, sécurité physique ; • organisationnel : procédures liées à la sécurité, suivi de la sécurité dans les contrats, en production, connaissance et application des règles les utilisateurs, …	*Catégorie de personnel (ex. Responsable de la SSI)*
7.1.2.2	Les services accessibles à des tiers, notamment via Internet, doivent faire l'objet de tests de vulnérabilités logiques fréquents. L'utilisation de services de détection automatisée de vulnérabilités logiques peut constituer une solution pour mener une surveillance quasi continue des vulnérabilités de ces services web. Ils ne se substituent cependant pas à une recherche de vulnérabilité menée par des experts de manière plus espacée.	*Catégorie de personnel*
7.1.2.3	La fréquence d'audit des vulnérabilités des différentes parties du SI doit être définie en fonction des enjeux identifiés par l'analyse de risques.	*Catégorie de personnel*
7.1.2.4	L'audit des vulnérabilités des parties externalisées peut être réalisé soit par les mêmes moyens, soit délégué à une tierce partie habilitée à intervenir par le prestataire. Tout test de vulnérabilité d'une partie hébergée du SI ne doit être réalisé qu'en totale conformité avec les modalités prévues au contrat avec le prestataire.	*Catégorie de personnel*

T7-1.3 Assurer un suivi de la disponibilité des ressources informatiques

Exigence :

⇒ La disponibilité des ressources du SI doit faire l'objet d'une planification et d'un suivi.

Déclinaison en règles :

Règles sur le suivi de la disponibilité des ressources du SI :

Réf.	Règles	Catégories de moyens du SI concernées
7.1.3.1	Un suivi de la disponibilité des ressources du SI doit être mis en place. Il doit porter en priorité sur : • le réseau local interne et l'accès Internet ; • les composants systèmes critiques du point de vue de leur disponibilité, identifiés suite à l'analyse de risques.	*Catégorie de personnel (ex. Responsable de la SSI, Responsable du service informatique)*
7.1.3.2	Le suivi doit permettre de : • vérifier régulièrement la conformité par rapport à la disponibilité attendue et d'identifier les écarts éventuels ; • prendre les actions correctives nécessaires.	*Catégorie de personnel*
7.1.3.3	Les capacités des ressources du SI doivent être gérées. Leur taux d'utilisation doit être suivi et les besoins d'extension de la capacité doivent être anticipés dans le cadre de l'utilisation habituelle du SI comme à l'occasion d'introduction de nouveaux composants et de l'évolution du nombre d'utilisateurs. La gestion des ressources du SI doit notamment porter sur : • les capacités des systèmes de stockage de données ; • les capacités de traitement, notamment des serveurs ; • les débits réseau (interne, accès Internet…) • le nombre de licences détenues (un nombre insuffisant de licences pouvant interdire l'usage d'applications à certains utilisateurs et les rendre indisponible pour eux)	*Equipements d'infrastructure système et réseau*

T7-2 Conserver les traces informatiques

T7-2.1 Tracer spécifiquement les actions réalisées sur les données de santé à caractère personnel et sur les autres données sensibles

Exigence :

⇒ Afin de garantir la traçabilité des accès aux données de santé et l'effectivité du droit d'opposition d'un usager au partage ou à l'échange de données de santé à caractère personnel le concernant, des traces doivent être générées et conservées par le SI pour tout accès, même en simple consultation, à des données de santé à caractère personnel.

⇒ La même exigence s'applique aux accès aux autres types de données sensibles.

Déclinaison en règles :

Règles sur les traces d'accès à des données de santé à caractère personnel :

Réf.	Règles	Catégories de moyens du SI concernées
7.2.1.1	La génération de traces doit être mise en place et activée pour toute application métier qui traite de données de santé à caractère personnel ou d'autres données sensibles, conformément aux guides d'utilisation et d'administration mis à disposition par les éditeurs des logiciels.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
7.2.1.2	Sauf spécificités mentionnées ici, les traces doivent être générées et gérées conformément aux règles de la thématique T7-2.2.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T7-2.2 Tracer les évènements informatiques

Exigence :

⇒ Les composants du SI doivent enregistrer sous forme de trace tout évènement susceptible de participer à la détection ou à la résolution d'un incident de sécurité du SI.

Déclinaison en règles :

Règles sur les traces générées par le SI :

Réf.	Règles	Catégories de moyens du SI concernées
7.2.2.1	Les fonctions de journalisation des évènements systèmes ou sécurité doivent être activées sur les différents composants d'infrastructure : serveurs, équipements réseau y compris Wifi, pare-feu, systèmes d'exploitation, application d'infrastructure (services DHCP, DNS, annuaire…), anti-virus, …	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
7.2.2.2	Les traces doivent comporter au minimum les informations suivantes :	*Equipements d'infrastructure*

	• date et heure de l'évènement ;
	• nature de l'évènement ;
	• équipement source de la trace (nom et adresse IP) ;
	• application source de la trace ;
	• toute autre information disponible et nécessaire à la description de l'évènement :
	  ○ identifiant de l'utilisateur,
	  ○ nature de l'opération réalisée,
	  ○ résultat de l'opération réalisée (succès, échec, erreur…),
	  ○ ...
		système et réseau, Equipements utilisateurs

7.2.2.3	Les horloges des différents équipements susceptibles de générer des traces doivent être synchronisées, par exemple à l'aide du protocole NTP.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
7.2.2.4	Les traces collectées constituent des informations à caractère personnel. Elles sont exclusivement destinées au suivi de la sécurité du SI et ne peuvent servir au contrôle de l'activité professionnelle ou extra-professionnelle des utilisateurs. Elles doivent être conservées de façon sécurisée et n'être accessibles qu'à un nombre restreint de personnes explicitement habilitées (typiquement le Responsable de la SSI). Il est recommandé qu'elles soient hébergées sur un serveur de stockage dédié à cet usage.	*Equipements d'infrastructure système et réseau (ex. Système de collecte et de stockage des traces)*
7.2.2.5	Sauf cas particulier (exigence légale ou réglementaire, ou autre) qui doit alors être documenté et justifié, les traces collectées doivent être conservées sur 12 mois glissants, puis être effacées.	*Equipements d'infrastructure système et réseau*
7.2.2.6	Les traces doivent être prises en compte dans le plan de sauvegarde afin qu'elles soient préservées en cas de d'incident.	*Equipements d'infrastructure système et réseau*
7.2.2.7	Les traces doivent être utilisées pour détecter rapidement et analyser les incidents de sécurité. A cette fin, une politique de gestion et d'analyse des traces devrait être élaborée sous le pilotage du Responsable de la SSI, avec la collaboration du Référent Incident SSI, afin de fixer les modalités de cette analyse, et mise en œuvre avec les moyens adéquats. L'utilisation d'outils d'analyse automatique des traces est généralement indispensable pour réaliser cette tâche d'analyse et de détection d'anomalies de sécurité. Les traces peuvent accessoirement être utilisées pour établir des statistiques qui doivent alors obligatoirement être anonymes (directement et indirectement) et pour détecter les flux anormaux sur le réseau.	*Catégorie de personnel (ex.* Responsable de la *SSI, Responsable du suivi opérationnel de la sécurité)*
7.2.2.8	Les utilisateurs du SI doivent être informés de la génération de traces à des fins d'exploitation du SI et de sécurité. Ils doivent être informés de leurs droits relatifs à ce traitement d'informations à caractère personnel. Cette information est typiquement réalisée via la Charte d'Utilisation des Ressources Informatiques.	*Catégorie de personnel (ex. Tout personnel utilisateur ou administrateur du SI)*

	La mise en place de la collecte de trace doit être effectuée en conformité avec les obligations légales et réglementaires, notamment en ce qui concerne la loi « Informatique et Libertés » et le droit du travail (information des instances de représentation du personnel…)	
7.2.2.9	Les interventions d'installation ou de maintenance sur les composants informatiques du SI devraient être tracées par le service informatique si elles ne donnent pas déjà lieu à la génération automatique de traces (comme c'est le cas par exemple pour les mises à jour automatiques des logiciels, de l'antivirus…). Ces traces doivent être accessibles au Responsable de la SSI pendant la durée spécifiée au 7.2.2.5 si elles comportent des informations à caractère personnel, et pendant la durée d'exploitation des composants concernés dans les autres cas.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
7.2.2.10	Tout accès d'administration à un composant informatique du SI devrait donner lieu à la génération d'une trace.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*

T7-3 Faire face à un incident de sécurité du SI

T7-3.1 Anticiper la survenue d'un incident de sécurité

Exigence :

⇒ La survenue d'un incident de sécurité doit être considérée comme un événement probable, voire certain. L'organisation nécessaire à la gestion de ce type de situation doit être définie et opérationnelle.

Déclinaison en règles :

Règles sur l'anticipation de la survenue d'un incident de sécurité :

Réf.	Règles	Catégories de moyens du SI concernées
7.3.1.1	Le Référent Incident SSI désigné en application de la règle 2.1.1.8 assure la coordination des actions liées aux incidents de sécurité.	*Catégorie de personnel (ex. Référent Incident SSI)*
7.3.1.2	Le Référent Incident SSI devrait identifier les experts techniques auxquels il peut recourir en cas d'incident de sécurité suspecté ou avéré, qu'il s'agisse de personnel interne (informaticien, juriste, …) ou de prestataire externe.	*Catégorie de personne*
7.3.1.3	Le Référent Incident SSI devrait établir, en coordination avec le Responsable de la SSI, le processus d'escalade de l'alerte afin de mobiliser les niveaux hiérarchiques adéquats de la structure et si nécessaire d'activer la cellule de crise.	*Catégorie de personne*
7.3.1.4	Le Référent Incident SSI devrait vérifier régulièrement l'efficacité des procédures de détection et de résolution d'incidents élaborées dans le cadre des règles 7.3.2.1 et	*Catégorie de personne*

	7.3.3.1. dans le cadre de tests techniques unitaires et d'exercices de mise en œuvre (simulation d'incident)	

T7-3.2 Détecter un incident de sécurité

Exigence :

⇒ Des moyens de détection des incidents de sécurité doivent être mis en place.

Déclinaison en règles :

Règles sur la détection des incidents de sécurité :

Réf.	Règles	Catégories de moyens du SI concernées
7.3.2.1	Le Référent Incident SSI doit coordonner la rédaction de procédures de détection d'incidents de sécurité par les personnes compétentes.	*Catégorie de personne (ex. Référent Incident SSI)*
7.3.2.2	Les utilisateurs du SI doivent être sensibilisés à la survenance potentielle d'incidents de sécurité, aux symptômes qu'ils sont susceptibles d'identifier dans leur utilisation du SI et à la procédure d'alerte qu'ils doivent mettre en œuvre dans ce cas (procédure qui doit être aussi simple que possible).	*Catégorie de personne*
7.3.2.3	Le Référent Incident SSI doit être informé de tout incident de production et de sa bonne résolution. L'accès doit être mis sur les incidents de production inhabituels ou dont les causes sont suspectes.	*Catégorie de personne (ex.* Personnel du service informatique, Responsable métier)

7.3.2.4	Il est recommandé que des moyens de détection d'anomalie de sécurité soient mis en œuvre afin d'alerter au plus vite le Référent Incident SSI :
	• console antivirus centralisée ;
	• dispositifs de contrôle d'intégrité des systèmes ;
	• dispositifs d'analyse automatique des traces ;
	• dispositif de détection d'intrusion réseau, dont
	  ○ détection de réponses ARP suspectes,
	  ○ détection de réponses DNS suspectes,
	  ○ détection d'annonces de routage suspectes ;
	• console de suivi des sauvegardes ;
	• etc.
		Equipements d'infrastructure système et réseau/Logiciels

T7-3.3 Prendre des mesures pour gérer les incidents de sécurité

Exigence :

⇒ Des procédures de réaction en cas d'incident de sécurité doivent être établies.

Déclinaison en règles :

Règles sur les mesures de gestion des incidents :

Réf.	Règles	Catégories de moyens du SI concernées
7.3.3.1	Le Référent Incident SSI devrait coordonner la rédaction de procédures de résolution d'incidents par les personnes compétentes. Des « fiches reflexe » peuvent également être élaborées pour des procédures très cadrées aux conditions de déclenchement claires et sans ambigüité.	*Catégorie de personnel (ex. Référent Incident SSI)*
7.3.3.2	Le Référent Incident SSI devrait participer à la résolution des incidents, en tirer des retours d'expérience, et le cas échéant établir avec le Responsable de la SSI des propositions de mesures à mettre en œuvre pour éviter qu'ils se répètent ou pour en limiter les impacts.	*Catégorie de personnel*

Le site de l'Agence Nationale de la Sécurité des Systèmes d'Information - www.ssi.gouv.fr - propose des informations pratiques dans la rubrique « Que faire en cas d'incident », qui peuvent être intégrés à vos procédures de gestion d'incidents de sécurité.

T7-4 Sauvegarder les données

Les enjeux de SSI liés à la sauvegarde des SI et la démarche permettant de définir un plan de sauvegarde sont détaillés dans le guide pratique « Règles de sauvegarde des Systèmes d'Information de Santé » [Réf. n°6.10] du corpus documentaire PGSSI-S. Les règles ci-dessous sont issues de ce guide pratique.

Ce document peut être utilement consulté pour plus d'informations sur le sujet.

T7-4.1 Organisation et Plan de sauvegarde

Exigence :

⇒ Un plan de sauvegarde du SI doit être établi et régulièrement testé.

Déclinaison en règles :

Règles sur le plan de sauvegarde du SI :

Réf.	Règles	Catégories de moyens du SI concernées
7.4.1.1	Le plan de sauvegarde doit identifier les besoins opérationnels métiers et d'infrastructure de sauvegarde et de restauration au minimum sur les points suivants : • définition du périmètre (systèmes, applications, données techniques, données de configuration, données métiers, documentation) à sauvegarder ; • définition du degré de confidentialité des sauvegardes ; • durée maximale admissible de restauration des données (DMARD) qui correspond au temps entre la demande de restauration et la restauration effective des données[14] ; • perte de données maximale admissible (PDMA) qui correspond au laps de temps maximal et admissible entre deux sauvegardes (perte des données modifiées pendant cette durée) ; • durée de conservation maximale des sauvegardes. La conservation des sauvegardes sur des longues périodes, au-delà de 5 ans, nécessite des précautions pour permettre une restauration en cas de besoin : régénération des sauvegardes pour s'affranchir de l'obsolescence des supports et du matériel de sauvegarde, et le cas échéant conservation de l'environnement matériel et logiciel.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
7.4.1.2	Le plan de sauvegarde devrait identifier, en conformité avec le périmètre de sauvegarde défini (règle 7.4.1.1),	*Equipements d'infrastructure*

[14] Dans le cadre des plans de continuité, cette notion est intégrée dans le délai d'indisponibilité maximale attendu (DIMA) qui correspond au temps entre le début de l'indisponibilité et la restauration effective, c'est-à-dire la DMARD à laquelle s'ajoute la durée entre le début d'une indisponibilité de données et sa détection ainsi que le délai entre la détection de l'indisponibilité et la demande de restauration des données.

	l'ensemble des composants informatiques du SI à inclure dans les processus de sauvegardes (ex. données, bases de données, applications et système d'exploitation des serveurs, des matériels médicotechniques, des équipements réseaux, serveurs, baies de stockage, serveurs de fichiers et postes de travail…). Le plan de sauvegarde devrait prendre en compte les liens entre les composants afin d'assurer la synchronisation et la cohérence des données lors des sauvegardes et restaurations. En particulier, lors des montées de versions de logiciel, il est important de sauvegarder la version précédente du logiciel afin de s'assurer du bon accès aux données en cas de restauration. Cette prise en compte peut notamment être réalisée par la sauvegarde de briques d'infrastructure complètes éventuellement associées à des plans de virtualisation du SI.	*système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
7.4.1.3	Pour chaque composant informatique identifié, le plan de sauvegarde décrit les procédures de sauvegarde à mettre en œuvre : • type de sauvegarde : sauvegarde complète, sauvegarde partielle, sauvegarde différentielle, sauvegarde incrémentale ; • périodicité de la sauvegarde (journalière, hebdomadaire, mensuelle…), périodicité de rotation des sauvegardes (exemple pour un SI : sauvegarde différentielle en semaine, sauvegarde complète le weekend, …) ; • contraintes de sauvegarde : sauvegarde à chaud, sauvegarde à froid, définition de la plage horaire de sauvegarde, ordonnancement des sauvegardes notamment entre les composants ayant des liens entre eux…	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
7.4.1.4	Le plan de sauvegarde doit identifier, pour chaque composant informatique, les procédures et les prérequis à la restauration. Les prérequis incluent les points suivants : • environnement de restauration (réseau, matériel de sauvegarde, serveur de restauration, ..) ; • caractéristiques des composants informatiques du matériel cible de la restauration ; • configurations logicielles (système d'exploitation, applications, …). Les procédures de restauration formalisent les points suivants : • diagnostic de la perte de données et détermination des données à récupérer en fonction des données perdues et des sauvegardes disponibles ; • mode de mise en œuvre de la récupération de données ; • modalités d'information des utilisateurs.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
7.4.1.5	Le plan de sauvegarde devrait prévoir le test des dispositions mises en œuvre pour assurer la sauvegarde.	*Equipements d'infrastructure*

	En pratique, les règles techniques concernant les sauvegardes, leur fréquence, leur restauration et la sécurité associée (règles des thématiques 7-4.2 à 7-4.5) doivent être testées régulièrement. Une campagne de test annuelle est recommandée.	*système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
7.4.1.6	Toute mise en production d'un nouveau système, d'une nouvelle application ou espace de données devrait faire l'objet d'une réflexion préalable sur sa sauvegarde et d'un ajout au plan de sauvegarde, validé par le responsable du SI.	*Equipements d'infrastructure système et réseau/Logiciels, Equipements utilisateurs/Logiciels*
7.4.1.7	Seul le personnel ou les sociétés désignées par le responsable du SI peuvent intervenir sur les processus de sauvegarde et de restauration des applications et des données.	*Catégories de personnel (ex. personnel du service informatique)*
7.4.1.8	Lorsque cela est permis par la charte utilisateur établie par l'établissement ou, au cas par cas, par le responsable du SI, les utilisateurs du SI sont autorisés à effectuer, sous leur propre responsabilité, des sauvegardes et restaurations des données de leur poste de travail dans le respect de la PSSI et de la charte informatique de la structure.	*Equipements utilisateurs/Logiciels*

T7-4.2 Règles techniques pour la sauvegarde des serveurs

Exigence :

⇒ Les serveurs du SI doivent faire l'objet de procédures de sauvegarde spécifiques répondant aux exigences de continuité de fonctionnement de ces composants centraux.

Déclinaison en règles :

Règles pour la sauvegarde des serveurs :

Réf.	Règles	Catégories de moyens du SI concernées
7.4.2.1	Une sauvegarde complète doit être effectuée avant chaque modification majeure d'un composant matériel ou logiciel (système ou application) et avant chaque changement majeur de configuration. Une sauvegarde complète doit être également effectuée après la modification si elle n'est pas déjà prévue dans le plan de sauvegarde.	*Equipements d'infrastructure système et réseau*
7.4.2.2	Pour chaque serveur de production, l'ensemble du paramétrage des systèmes d'exploitation et des applications (comptes et droits utilisateurs, paramètres métier, …) doit être sauvegardé selon les besoins de disponibilité définis par les responsables de traitement à une fréquence minimum déterminée en fonction des besoins et contraintes. A titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'éléments.	*Equipements d'infrastructure système et réseau*
7.4.2.3	Pour chaque serveur de production, l'ensemble des données des applications métier doit être sauvegardé selon les besoins de disponibilité définis par les	*Equipements d'infrastructure système et réseau*

	responsables de traitement à une fréquence minimum déterminée en fonction des besoins et contraintes. A titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'élément.	
7.4.2.4	Pour chaque serveur de production, les différentes versions des programmes (systèmes, bases de données et applications) doivent être sauvegardées et les supports conservés, tant que les données de l'application sont susceptibles d'être restaurées. En effet, si des données un peu anciennes sont restaurées, il est possible qu'il soit nécessaire de restaurer ces données dans un environnement nécessitant des versions des logiciels et systèmes antérieures aux versions actuelles de production.	*Equipements d'infrastructure système et réseau*
7.4.2.5	Une vérification systématique des sauvegardes est réalisée en fin de procédure. Pour les bases de données, une opération de restauration à blanc peut être planifiée en plus des tests prévus dans le cadre de la règle 7.4.5.2.	*Equipements d'infrastructure système et réseau*
7.4.2.6	L'ensemble des opérations de sauvegarde est journalisé. Les journaux sont conservés avec les supports de sauvegardes. Ces derniers comportent au minimum les informations suivantes : • références du dispositif de sauvegarde ; • périmètre ou composants concernés ; • type de sauvegarde ; • fichiers sauvegardés hors VM; • date de la sauvegarde ; • statut de la sauvegarde.	*Equipements d'infrastructure système et réseau*

T7-4.3 Règles techniques pour la sauvegarde des postes de travail

Exigence :

⇒ Les postes de travail du SI doivent faire l'objet de procédures de sauvegarde spécifiques pour prendre en compte les éventuelles modalités particulières d'utilisation de ces équipements.

Déclinaison en règles :

Règles pour la sauvegarde des postes de travail :

Réf.	Règles	Catégories de moyens du SI concernées
7.4.3.1	Dans le cas d'une utilisation monoposte, une sauvegarde complète devrait être effectuée avant chaque modification majeure d'un composant matériel ou logiciel (système ou application) et avant chaque changement majeur de configuration. Une sauvegarde complète devrait être également effectuée après la modification si elle n'est pas déjà prévue dans le plan de sauvegarde.	*Equipements utilisateurs*
7.4.3.2	Dans le cas d'un exercice individuel ou si la charte utilisateur de l'établissement permet le stockage de données métiers sur les postes de travail, la sauvegarde de l'ensemble des données des applications métier doit être planifiée en fonction des besoins de disponibilité des données définis par les responsables de traitement. A titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'éléments.	*Equipements utilisateurs*
7.4.3.3	Une vérification systématique des sauvegardes devrait être réalisée en fin de procédure.	*Equipements utilisateurs*

T7-4.4 Règles techniques générales pour la sauvegarde

Exigence :

⇒ Les procédures opérationnelles de sauvegarde doivent garantir la sécurité des données sauvegardées.

Déclinaison en règles :

Règles générales pour la sauvegarde :

Réf.	Règles	Catégories de moyens du SI concernées
7.4.4.1	Les dispositifs de sauvegarde devraient faire l'objet d'un contrat de maintenance matérielle et logicielle adapté aux besoins de disponibilité du SI.	*Equipements d'infrastructure système et réseau (ex. système de sauvegarde centralisée)*
7.4.4.2	Chaque support amovible de sauvegarde doit être identifié et étiqueté avec a minima son identifiant, et devrait comporter sa date de mise en première circulation et sa date de péremption.	*Equipements utilisateurs/Support de données amovibles (ex. bande de sauvegarde)*

7.4.4.3	Un jeu de supports, correspondant à une sauvegarde complète, devrait régulièrement être stocké dans un espace protégé contre les menaces physiques et environnementales (vols, saccages, incendies, dégâts des eaux, perturbations magnétiques, …) et physiquement éloigné des composants du SI sauvegardés. Cet éloignement physique devrait garantir qu'un même incident ne peut affecter à la fois les composants sauvegardés et leur sauvegarde. Le lieu de « stockage éloigné » devrait être approprié au type de structure. Ce lieu pourra être, par exemple, un site secondaire de l'organisme, un coffre de banque, etc. Il est recommandé qu'une sauvegarde hebdomadaire soit stockée sur un lieu distant.	*Equipements utilisateurs/Support de données amovibles*
7.4.4.4	Les supports de sauvegarde devraient être protégés en conformité avec les règles de la thématiques T3-1.3. Le niveau de protection des sauvegardes devrait être au moins identique à celui des éléments sauvegardés. En particulier, l'accès aux sauvegardes devrait faire l'objet d'un contrôle et d'une restriction d'accès aux seuls intervenants autorisés par le responsable de traitement que ce soit lors de leur manipulation, au cours des sauvegardes-restaurations, sur les lieux de stockage ou pendant les opérations de transport. A cet effet, il est possible de mettre en œuvre des solutions de chiffrement des données afin de réduire les risques d'accès aux données par des personnes non autorisées notamment en cas de perte de supports de stockage. Il est alors essentiel que les clés nécessaires au déchiffrement des sauvegardes soient également sauvegardées et que ces sauvegardes soient protégées et conservées séparément par une personne autorisée. Le lecteur pourra se référer au Référentiel Général de Sécurité (RGS [Réf. n°9]) qui comporte une annexe décrivant les exigences relatives à la fonction de sécurité « confidentialité »[15]	*Equipements utilisateurs/Support de données amovibles*
7.4.4.5	Tous les supports de sauvegarde devraient, avant leur réutilisation dans un autre contexte ou leur mise au rebut, faire l'objet d'une campagne systématique d'effacement physique ou, à défaut, être physiquement détruits. La destruction des données stockées sur les supports de sauvegarde devrait être réalisée en conformité avec les règles de la thématique T3-1.4.	*Equipements utilisateurs/Support de données amovibles*
7.4.4.6	Si la sauvegarde de données sensibles (données à caractère personnel, paramétrages d'équipement parmi lesquels peuvent se trouver des mots de passe…) est réalisée via le réseau, ces données ne devraient transiter par le réseau que sous forme chiffrée.	*Equipements d'infrastructure système et réseau (ex. système de sauvegarde centralisée)*
7.4.4.7	Quand les besoins métiers le nécessitent, un mécanisme de contrôle d'intégrité des données sauvegardées peut être mis en place.	*Equipements d'infrastructure système et réseau*

[15] http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html

	Si ce contrôle d'intégrité vise à détecter une éventuelle falsification des données, il est recommandé d'utiliser la fonction de hachage SHA-256 pour réaliser une empreinte des données sauvegardée, voire une signature électronique. Ces empreintes devront être protégées et conservées séparément des sauvegardes.	*(ex. système de sauvegarde centralisée)*

T7-4.5 Règles relatives à la restauration et au contrôle des sauvegardes

Exigence :

⇒ Un contrôle de la qualité des supports de sauvegarde et du résultat des opérations de restauration doit être systématiquement effectué.

Déclinaison en règles :

Règles relatives à la restauration et au contrôle des sauvegardes :

Réf.	Règles	Catégories de moyens du SI concernées
7.4.5.1	Tous les supports de sauvegarde devraient faire l'objet d'une surveillance périodique pour garantir leur efficacité physique, que ce soit par échantillonnage et test de restauration à blanc de sauvegardes anciennes, ou par suivi des paramètres techniques de bas niveau (erreurs de lecture, corrigées ou non) à l'occasion d'opérations de restauration. En cas d'incident lié à la qualité du support lors d'une opération de sauvegarde ou de restauration, comme en cas de suspicion de défaut, le support incriminé devrait être mis au rebut.	*Equipements utilisateurs/Support de données amovibles (ex. bande de sauvegarde)*
7.4.5.2	Des tests de restauration sont menés de manière régulière. Une fréquence de test annuelle est recommandée.	*Equipements utilisateurs/Support de données amovibles (ex. bande de sauvegarde)*
7.4.5.3	Chaque opération de restauration doit donner lieu à une vérification du bon fonctionnement du composant restauré et de la sécurité. En particulier, le contrôle d'accès aux éléments restaurés doit être cohérent avec celui mis en œuvre pour les éléments initiaux sauvegardés. Le résultat de cette vérification est consigné dans une fiche de restauration qui comporte les informations suivantes : • opérateur de sauvegarde ; • demandeur de la restauration ; • fichiers restaurés ; • date de la sauvegarde ; • date de restauration ; • statut des vérifications effectuées.	*Equipements d'infrastructure système et réseau, Equipements utilisateurs*
7.4.5.4	En fonctionnement habituel, les exploitants doivent utiliser leur compte nominatif pour effectuer des opérations de restauration ou de contrôle des sauvegardes.	*Catégories de personnel (ex. personnel du service informatique)*

	Toutefois, il peut exister un compte administrateur du système de sauvegarde. Ce compte ne doit pas être un compte par défaut du système. L'identifiant et le mot de passe durci associés à ce compte doivent être consignés dans un coffre-fort (physique ou électronique) à mots de passe. Il ne doit être utilisé qu'en cas de force majeure (indisponibilité des exploitants usuels notamment), sous le contrôle du responsable du SI.	

T7-4.6 Règles relatives aux contrats d'externalisation des sauvegardes

Exigence :

⇒ Les contrats d'externalisation des sauvegardes doivent intégrer les clauses requises pour garantir une protection adéquate des données sauvegardées.

Déclinaison en règles :

Règles générales pour la sauvegarde :

Réf.	Règles	Catégories de moyens du SI concernées
7.4.6.1	Un contrat d'externalisation des opérations ou des supports de sauvegarde ne devrait être signé avec un prestataire que s'il est agréé ou certifié pour l'hébergement des données de santé à caractère personnel, pour ce type de service.	*Organisation (ex. prestataire d'externalisation des opérations ou des supports de sauvegarde)*
7.4.6.2	Le contrat d'externalisation des opérations ou des supports de sauvegarde devrait se conformer aux règles 6.6.6.1 et 6.6.6.2.	*Organisation*

T7-5 Mettre en place un Plan de Continuité Informatique

Les enjeux de SSI liés à la définition d'un Plan de Continuité Informatique et la démarche permettant de définir un tel plan sont détaillés dans le guide pratique « Plan de Continuité Informatique – Principes de base » [Réf. n°6.4] du corpus documentaire PGSSI-S.

Le lecteur se rapportera à ce document pour une première approche sur l'élaboration d'un Plan de Continuité Informatique de sa structure.

T7-5.1 Définir l'organisation nécessaire au Plan de Continuité Informatique

Exigence :

⇒ L'organisation nécessaire à l'élaboration, la mise en application et la maintenance du Plan de Continuité Informatique devrait être formalisée.

Déclinaison en règles :

Règles pour l'organisation liée au Plan de Continuité Informatique :

Réf.	Règles	Catégories de moyens du SI concernées
7.5.1.1	L'élaboration, la mise en application, la maintenance et les tests du Plan de Continuité Informatique devraient être pilotés par la personne en charge de la fonction « Référent Plan de Continuité Informatique » désigné en application de la règle 2.1.1.10.	*Catégorie de personnel (ex. Référent PCI, Référent PCA)*
7.5.1.2	Le Référent Plan de Continuité Informatique (Référent PCI) devrait tenir le Responsable de la SSI informé de l'élaboration, de la mise en application, de la maintenance et des tests du PCI.	*Catégorie de personnel*

T7-5.2 Elaborer le Plan de Continuité Informatique

Exigence :

⇒ Un Plan de Continuité Informatique doit être établi en cohérence avec le Plan de Continuité d'Activité (PCA) de la structure.

Déclinaison en règles :

Règles d'élaboration du Plan de Continuité Informatique :

Réf.	Règles	Catégories de moyens du SI concernées
7.5.2.1	Un Plan de Continuité Informatique devrait être établi afin de répondre aux exigences de continuité établies par le Plan de Continuité d'Activité (PCA) de la structure en cas de réalisation de l'un des incidents envisagés dans ce PCA.	*Catégorie de personnel (ex. Référent PCI, Référent PCA)*
7.5.2.2	Le Plan de Continuité Informatique devrait être élaboré en cohérence avec le PCA afin de : • tenir compte des différents modes de fonctionnement dégradés et de secours envisagés par les métiers ;	*Catégorie de personnel*

	• vérifier que le PCA prend bien en compte les prérequis spécifiques au rétablissement du fonctionnement du SI attendu (locaux de repli, personnel nécessaire, logistique, …).	

T7-5.3 Tester le Plan de Continuité Informatique

Exigence :

⇒ Le Plan de Continuité Informatique devrait être régulièrement testé.

Déclinaison en règles :

Règles générales pour le test du Plan de Continuité de fonctionnement :

Réf.	Règles	Catégories de moyens du SI concernées
7.5.3.1	La pertinence et l'efficacité du Plan de Continuité Informatique et de sa mise en œuvre effective devraient être régulièrement testées dans le cadre : • de tests internes au SI ; • d'exercices de mise en œuvre du PCA de la structure.	*Ensemble du SI*

Thématique 8 : Annexes

Annexe 1 - Fonctions sécurité numérique et RGPD

Nom de la fonction	Responsable
Responsable de la Sécurité des SI Référent Incident SSI (CHU & GHT)	Julien ROUSSELLE
Responsable Infrastructure CHU	Pascal TOURBIER
Responsable Convergence Infrastructure et du SMSI (CHU & GHT) Référent PCI	Yann DELAHAYE
RIL CHU	Valérie MARSEILLE
DPO (CHU & GHT)	Dr Paulo HENRIQUES Dr Yves JOUCHOUX (ex DPO)
DSN et RSI (CHU & GHT)	Sébastien FLOREK Sylvain CHAMBEAU

Il existe également un tableau imposé par la certification avec les correspondants dans chaque établissement du GHT SLS : référents informatiques, sécurité, RGPD, CIV, DIM, DG.

Annexe 2 - Durée de conservation

Type de donnée à caractère personnel	Durée de conservation

FINALITE DU TRAITEMENT	DUREE DE CONSERVATION
RESSOURCES HUMAINES	
Gestion du personnel	5 ans (en archivage intermédiaire) à compter du départ du salarié.
Gestion de la paie	5 ans à compter du versement de la paie
Fichiers de recrutement	Destruction immédiate si le candidat n'est pas retenu ni pour le poste à pourvoir ni dans le cadre d'un futur recrutement Possibilité de conserver le CV pendant 2 ans après le dernier contact avec le candidat
Vidéosurveillance	1 mois
Gestion des réunions instances représentatives du personnel	Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heure de délégation ne sont pas conservées au delà de la période de sujétion de l'employé concerné
Gestion de l'annuaire du personnel	Les données ne sont pas conservées au delà de la période d'emploi de la personne concernée
Gestion des œuvres sociales et culturelles	Les données sont conservées tant que la personne travaille pour l'établissement ou jusqu'à ce qu'elle en demande la suppression
Contrôle de l'utilisation d'internet par les salariés	6 mois concernant l'historique des connexions
Contrôle de l'utilisation de la messagerie (outil de mesure de la taille, de la fréquence, analyse des pièces jointes, etc…)	6 mois
Gestion de la téléphonie (données relatives à l'utilisation des services de téléphonie : numéros appelés, numéros entrants, etc…)	1 an
Géolocalisation des véhicules professionnels	2 mois (historique des déplacements)
Contrôle des horaires	Les éléments d'identification ne doivent pas être conservés au-delà de 5 ans après le départ du salarié. Les informations relatives aux horaires des salariés peuvent être conservées pendant 5 ans. La conservation des données relatives aux motifs d'absence est limitée à une durée de 5 ans
Gestion de la restauration	En cas de paiement direct ou de prépaiement des repas les données monétique ne peuvent pas être conservées plus de 3 mois. En cas de paiement par retenue sur salaire, la durée de conservation est de 5 ans.

Contrôle d'accès	Les éléments d'identification ne doivent pas être conservés au-delà du temps pendant lequel la personne est habilitée à pénétrer dans les locaux concernés. 3 mois (historique des passages)
Sanctions disciplinaires	3 ans glissant sauf amnistie
Enregistrement des conversations téléphoniques	2 mois glissant
Autocommutateur (détail des appels téléphoniques)	6 mois glissant
Mandat des représentants des personnels (nature du mandat et syndicat d'appartenance)	6 mois après la fin du mandat
SANTE	
Dossier médical dans les cabinets libéraux	10 ans
Dossier médical dans les établissements de santé publics et privés	Conservation du dossier pendant 20 ans à compter du dernier passage (séjour ou consultation). Si la durée de conservation s'achève avant le 28ème anniversaire du patient, son dossier est conservé jusqu'à cette date. Si le patient décède moins de 10 ans après son dernier passage, le dossier est conservé pendant une durée de 10 ans après son décès.
Télétransmission des feuilles de soins	Conservation des doubles et AR pendant 90 jours
Gestion de la pharmacie, dispensation des médicaments, produits de santé, DM…	Conservation des données enregistrées sur le patient pendant 3 ans à compter de la dernière intervention sur son dossier. A l'issue de ce délai les données sont archivées pendant 15 ans. Conservation de l'ordonnancier pendant 10 ans. Conservation du registre des stupéfiants pendant 10 ans à partir de sa dernière mention. Conservation du registre des médicaments dérivés du sang pendant 40 ans.
Gestion des laboratoires d'analyse médicale	Conservation des données enregistrées sur le patient pendant 5 ans à compter de la dernière intervention sur son dossier. A l'issue de ce délai les données sont archivées pendant 10 ans. Pour les laboratoires en établissement de santé, conservation pendant 20 ans des dossiers et registres.
	Détermination de la durée de conservation au cas par cas suivant le principe de proportionnalité. La durée de conservation est à déterminer en fonction de la finalité poursuivie et des catégories de données traitées. La durée de conservation doit

Recherche médicale	être très courte, les données anonymisées ou pseudo anonymisées.
Analyse des pratiques ou des activités de soins et de prévention	Durée de conservation très courte, qui ne dépasse pas 2 ans dans la plupart des cas. Durée proportionnelle à la finalité de l'étude, conservée le temps de l'étude et supprimée dès la fin de l'étude.

✍ La durée de conservation de chaque type de données à caractère personnel dépend de la finalité des traitements pour lesquelles elles ont été collectées.

En règle générale :

- La durée de conservation des données à caractère personnel déconnectées de la prise en charge sanitaire de patients (ex. données concernant les fournisseurs, les employés, les prestataires…) est variable et découle des exigences légales et règlementaires applicables au domaine et aux données considérés.

  Quand une durée de conservation n'est pas imposée de cette manière, la durée doit être fixée de façon proportionnée aux finalités recherchées, et doit se conformer aux recommandations de la CNIL. En particulier, la durée de conservation après la dernière utilisation des données doit être fixée au minimum nécessaire, et ne doit pas dépasser 6 mois sans une justification étayée.

- Le dossier médical constitué pour chaque patient hospitalisé (y compris les données à caractère personnel, même dans le cas où ce ne sont pas des données de santé à caractère personnel, comme *par* exemple les coordonnées du représentant légal) doit être conservé par les structures de santé, publiques et privées, pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans la structure ou de sa dernière consultation au sein de l'établissement.

En l'absence de règles propres au dossier constitué par une structure pour le suivi de ses patients, il est d'usage d'adopter la même durée de conservation.

Cas particuliers les plus fréquents :

- Le dossier médical constitué pour un patient de moins de 8 ans lors du son dernier passage doit être conservé pendant une durée de vingt-huit années. (Cf. article R1112-7 du code de la santé publique).
- En cas de décès le dossier médical est conservé pendant 10 ans à compter de la date du décès. (Cf. article R1112-7 du code de la santé publique).
- Les délais de conservation des dossiers médicaux sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison de leurs interventions au sein de l'établissement. (Cf. article R1112-7 du code de la santé publique).

☞ Le guide PGSSI-S sur l'archivage présente une synthèse des principales règlementations permettant de définir la durée de conservation de données dans des cas spécifiques qui ne correspondent pas au cas général. Il constitue un bon point de départ pour identifier les éventuelles spécificités en termes de durée de conservation de données qui pourraient s'appliquer à votre structure. Toutefois, il ne saurait se substituer à la veille règlementaire décrite dans le thème T1-4 qui doit être l'occasion de réinterroger régulièrement les durées de conservation identifiées dans cette annexe.

Annexe 3 - Correspondance entre thématiques PSSI et HN, PSSIE et ISO27002

Correspondance entre thématiques PSSI et les actions pour atteindre les prérequis du programme Hôpital Numérique

Thème	**Intitulé du thème, sous-thème ou exigence de la PSSI** *(limité aux sous-thèmes auxquels correspond au moins une action pour atteindre les prérequis HN)*	**Actions pour atteindre les prérequis HN – Octobre 2012** (voir [Réf. n°3bis])
1	**Répondre aux obligations légales**	
1.1	**Respecter les principes de la protection des données à caractère personnel**	
1.1.1	Respecter les procédures préalables devant la CNIL	P3.3-1,2,3
1.1.2	Sensibiliser le personnel aux enjeux concernant les données à caractère personnel	P3.1-5, P3.3-1,2,3,
1.1.3	Respecter les droits des personnes	P3.3-1,2,3
1.2	**Respecter les règles d'échange et de partage de données de santé à caractère personnel**	
1.2.1	Informer l'usager et recueillir son consentement	P3.3-1,2,3
1.2.2	Limiter l'accès aux données de santé à caractère personnel aux personnes participant à la prise en charge	P3.3-1,2,3,
2	**Promouvoir et organiser la sécurité**	
2.1	**Définir une organisation pour la mise en œuvre de la SSI au sein de la structure**	
2.1.1	Identifier les acteurs de la politique de sécurité de la structure et leurs activités	P3.1-1,2,3,4
2.1.2	Formaliser les remontées d'informations sur la sécurité à la direction	
2.2	**Faire connaître les principes essentiels de sécurité informatique**	
2.2.1	Sensibiliser, former et responsabiliser le personnel	P3.1-5, P3.2-1,2,3
2.2.2	Décliner les règles de la PSSI dans les procédures opérationnelles	P3.1-5
4	**Protéger les infrastructures informatiques**	
4.1	**Maîtriser le parc informatique**	
4.1.1	Identifier physiquement chaque équipement informatique ou dispositif médical connecté détenu par la structure	P3.1-4
4.1.2	Identifier les composants logiciels du SI	P3.1-4
4.1.3	Identifier les services d'infrastructure du SI	P3.1-4
4.1.4	Vérifier régulièrement la complétude du recensement et les licences	P3.1-5
4.1.5	Documenter le SI	
5	**Maîtriser les accès aux informations**	

Thème	**Intitulé du thème, sous-thème ou exigence de la PSSI** *(limité aux sous-thèmes auxquels correspond au moins une action pour atteindre les prérequis HN)*	**Actions pour atteindre les prérequis HN – Octobre 2012** (voir [Réf. n°3bis])
5.1	**Accorder les accès aux informations aux seules personnes dûment autorisées**	
5.1.1	Formaliser des règles d'accès aux informations	P3.4-1
5.1.2	Gérer les accès aux informations	
5.1.3	Contrôler régulièrement les droits d'accès	
5.2	**Adopter les bonnes pratiques en matière d'authentification des utilisateurs**	
5.2.1	Créer des comptes qui respectent les bons usages	P3.4-2,3
5.2.2	Utiliser les dispositifs d'authentification en respectant les consignes de sécurité	P3.4-2,3
5.2.3	Protéger les comptes contre les tentatives d'usurpation d'identité	
5.2.4	Protéger les comptes des services et les comptes administrateurs techniques par défaut	
7	**Limiter la survenue et les conséquences d'incidents de sécurité du SI**	
7.1	**Vérifier le niveau de sécurité des moyens informatiques**	
7.1.1	Procéder à un contrôle régulier de la bonne mise en œuvre des règles de la PSSI	P3.1-5
7.1.2	Procéder à un audit régulier des vulnérabilités du SI	P3.1-5
7.1.3	Assurer un suivi de la disponibilité des ressources informatiques	P2.2-1,2,3
7.2	**Conserver les traces informatiques**	
7.2.1	Tracer spécifiquement les actions réalisées sur les données de santé à caractère personnel et sur les autres données sensibles	P3.5-1,2,3
7.2.2	Tracer les évènements informatiques	P3.5-1,2,3
7.4	**Sauvegarder les données**	
7.4.1	Organisation et Plan de sauvegarde	P2.1-3
7.4.2	Règles techniques pour la sauvegarde des serveurs	P2.1-3
7.4.3	Règles techniques pour la sauvegarde des postes de travail	P2.1-3
7.4.4	Règles techniques générales pour la sauvegarde	P2.1-3
7.4.5	Règles relatives à la restauration et au contrôle des sauvegardes	P2.1-3
7.4.6	Règles relatives aux contrats d'externalisation des sauvegardes	P2.1-3
7.5	**Mettre en place un Plan de Continuité Informatique**	
7.5.1	Définir l'organisation nécessaire au Plan de Continuité Informatique	P2.1-1,2,3,4,5, P2.3-1,2,3,4,5
7.5.2	Elaborer le Plan de Continuité Informatique	P2.1-1,2,3,4,5, P2.3-1,2,3,4,5

Thème	Intitulé du thème, sous-thème ou exigence de la PSSI *(limité aux sous-thèmes auxquels correspond au moins une action pour atteindre les prérequis HN)*	Actions pour atteindre les prérequis HN – Octobre 2012 (voir [Réf. n°3bis])
7.5.3	Tester le Plan de Continuité Informatique	P2.1-1,2,3,4,5, P2.3-1,2,3,4,5

Correspondance entre thématiques PSSI et objectifs de sécurité PSSIE

La correspondance au niveau individuel des règles du canevas de PSSI et des règles de la PSSIE est présentée dans le document « Annexe au canevas de PSSI pour les structures des secteurs sanitaire et médico-social : Couverture des règles de la PSSIE par les règles du canevas de PSSI » [Réf. n°6.1bis]

Thème	Intitulé du thème, sous-thème ou exigence de la PSSI	Objectifs de sécurité PSSIE – Version 1.0 (voir [Réf. n°10])
1	**Répondre aux obligations légales**	
1.1	**Respecter les principes de la protection des données à caractère personnel**	
1.1.1	Respecter les procédures préalables devant la CNIL	Obj. 10
1.1.2	Sensibiliser le personnel aux enjeux concernant les données à caractère personnel	Obj. 19
1.1.3	Respecter les droits des personnes	
1.2	**Respecter les règles d'échange et de partage de données de santé à caractère personnel**	
1.2.1	Informer l'usager et recueillir son consentement	
1.2.2	Limiter l'accès aux données de santé à caractère personnel aux personnes participant à la prise en charge	Obj. 2, 4, 19
1.3	**Répondre aux obligations de conservation et de restitution des données**	
1.3.1	Fixer une durée de conservation des données à caractère personnel	
1.3.2	Respecter les règles relatives à l'hébergement de données de santé à caractère personnel	Obj. 19
1.4	**Veille réglementaire**	
1.4.1	Assurer une veille réglementaire des dispositions applicables à la structure en matière de SSI	
2	**Promouvoir et organiser la sécurité**	
2.1	**Définir une organisation pour la mise en œuvre de la SSI au sein de la structure**	
2.1.1	Identifier les acteurs de la politique de sécurité de la structure et leurs activités	Obj. 1, 5, 24, 33
2.1.2	Formaliser les remontées d'informations sur la sécurité à la direction	Obj. 1, 6
2.2	**Faire connaître les principes essentiels de sécurité informatique**	
2.2.1	Sensibiliser, former et responsabiliser le personnel	Obj. 2, 4, 19, 23

Thème	Intitulé du thème, sous-thème ou exigence de la PSSI	Objectifs de sécurité PSSIE – Version 1.0 (voir [Réf. n°10])
2.2.2	Décliner les règles de la PSSI dans les procédures opérationnelles	Obj. 2, 4, 10, 19, 21, 22, 23, 24
3	**Assurer la sécurité physique des équipements informatiques du SI**	
3.1	**Maîtriser l'accès aux équipements du SI qui sont nécessaires à l'activité de la structure et assurer leur protection physique**	
3.1.1	Assurer la protection physique des équipements informatiques d'infrastructure du SI qui contiennent des données sensibles	Obj. 9, 10, 19
3.1.2	Assurer la protection physique des postes de travail qui contiennent des données sensibles	Obj. 9, 19, 23, 25
3.1.3	Assurer la protection physique des équipements amovibles qui contiennent des données sensibles	Obj. 19, 23
3.1.4	Assurer la destruction de données lors du transfert de matériels informatiques	Obj. 19, 22, 23, 24, 25
4	**Protéger les infrastructures informatiques**	
4.1	**Maîtriser le parc informatique**	
4.1.1	Identifier physiquement chaque équipement informatique ou dispositif médical connecté détenu par la structure	Obj. 3, 23, 24, 25
4.1.2	Identifier les composants logiciels du SI	Obj. 3
4.1.3	Identifier les services d'infrastructure du SI	Obj. 3, 17
4.1.4	Vérifier régulièrement la complétude du recensement et les licences	Obj. 3, 9, 23, 28
4.1.5	Documenter le SI	Obj. 3, 6, 17, 20
4.2	**Gérer le réseau local**	
4.2.1	Identifier ou authentifier chaque équipement connecté au SI	Obj. 12, 16, 23, 24
4.2.2	Cloisonner les réseaux selon les besoins de sécurité	Obj. 3, 4, 9, 13, 18, 19, 22, 23, 24, 25
4.3	**Gérer la connexion Internet**	
4.3.1	Sécuriser la connexion Internet	Obj. 12, 14, 16, 18, 23, 31
4.3.2	Limiter les accès Internet en conformité avec la Charte d'Utilisation des Ressources Informatiques	
4.3.3	Conserver une trace des connexions Internet	
4.4	**Gérer les connexions sans fil**	
4.4.1	Sécuriser la mise en place d'un point d'accès Wifi	Obj. 15, 16, 25
4.4.2	Assurer l'exploitation d'un point d'accès Wifi	Obj. 15
4.4.3	Sécuriser la mise en place d'un point d'accès Wifi "invité"	Obj. 15
4.5	**Protéger l'accès aux systèmes**	
4.5.1	Gérer les mots de passe pour qu'ils présentent une robustesse appropriée	Obj. 2, 4, 19, 21, 22, 27, 30

Thème	Intitulé du thème, sous-thème ou exigence de la PSSI	Objectifs de sécurité PSSIE – Version 1.0 (voir [Réf. n°10])
4.5.2	Verrouiller les postes de travail	Obj. 19, 20, 22
4.5.3	Assurer la protection logique des équipements informatiques	Obj. 16, 19, 20, 22, 24, 25, 26, 27, 31
4.5.4	Vérifier l'authenticité des logiciels	Obj. 19, 20, 22
4.5.5	Procéder à une mise à niveau régulière des moyens informatiques	Obj. 19, 20, 22, 24, 31
4.5.6	Assurer la protection logique des supports informatiques et équipements mobiles qui contiennent des données sensibles	Obj. 4, 19, 20, 22, 23, 24, 25
5	**Maîtriser les accès aux informations**	
5.1	**Accorder les accès aux informations aux seules personnes dûment autorisées**	
5.1.1	Formaliser des règles d'accès aux informations	Obj. 19, 21, 22, 24, 25
5.1.2	Gérer les accès aux informations	Obj. 19, 21, 22, 25
5.1.3	Contrôler régulièrement les droits d'accès	Obj. 2, 19, 21, 22
5.2	**Adopter les bonnes pratiques en matière d'authentification des utilisateurs**	
5.2.1	Créer des comptes qui respectent les bons usages	Obj. 19, 21, 22, 25
5.2.2	Utiliser les dispositifs d'authentification en respectant les consignes de sécurité	Obj. 19, 21, 22
5.2.3	Protéger les comptes contre les tentatives d'usurpation d'identité	Obj. 19, 21, 22, 30
5.2.4	Protéger les comptes des services et les comptes administrateurs techniques par défaut	Obj. 16, 19, 21, 22, 25
5.3	**Lutter contre les accès non autorisés**	
5.3.1	Utiliser des moyens garantissant la sécurité des échanges	Obj. 12, 16, 19, 21, 22, 23, 24
6	**Acquérir des équipements, logiciels et services qui préservent la sécurité du SI**	
6.1	**Mettre en œuvre des prestations de télésurveillance, télémaintenance ou téléassistance**	
6.1.1	Encadrer la prestation par un contrat conforme aux règles du guide pratique « PGSSI-Règles d'intervention à distance »	Obj. 8, 22
6.1.2	Mettre en œuvre des dispositions techniques de sécurité spécifiques dans le SI	Obj. 8, 22
6.2	**Acquérir des dispositifs connectés**	
6.2.1	Demander aux industriels et fournisseurs un engagement de conformité au guide pratique « PGSSI-Dispositifs connectés »	
6.2.2	Obtenir un accès aux documentations requises par le guide pratique « PGSSI-Dispositifs connectés »	
6.2.3	Identifier les solutions de réversibilité permettant une reprise des données	

Thème	Intitulé du thème, sous-thème ou exigence de la PSSI	Objectifs de sécurité PSSIE – Version 1.0 (voir [Réf. n°10])
6.3	**Acquérir des progiciels « sur étagère »**	
6.3.1	Demander aux industriels et fournisseurs un engagement de conformité au guide pratique « Accès Tiers » en cas d'applicabilité	Obj. 24, 29, 30, 31
6.3.2	Vérifier les fonctionnalités de sécurité au regard de la PSSI	Obj. 29, 30
6.4	**Acquérir des équipements informatiques**	
6.4.1	Demander aux industriels et fournisseurs un engagement de conformité au guide pratique « Destruction de données lors de transferts de matériels informatiques »	
6.5	**Encadrer les développements spécifiques et les acquisitions de logiciels, d'équipements du SI et d'équipements connectés**	
6.5.1	Intégrer la SSI dans les cahiers des charges	Obj. 5, 6, 7, 19, 22, 24, 29, 30
6.5.2	Valider les nouveaux composants du SI avant leur mise en production	Obj. 5, 6, 14, 29, 30
6.5.3	Assurer la formation aux nouveaux composants du SI	Obj. 30
6.6	**Définir l'objet des prestations et les limites d'engagement dans les relations contractuelles avec les tiers fournisseurs de service**	
6.6.1	Définir précisément dans les contrats le contenu des prestations confiées aux tiers fournisseurs de service pour répondre aux obligations de sécurité	Obj. 8, 10
6.6.2	S'assurer de la capacité de restitution des données de santé à caractère personnel , et plus généralement de toute donnée confiée, sous une forme réutilisable par la structure	Obj. 8, 10
6.6.3	Clauses de sécurité en cas d'externalisation de la destruction des données	Obj. 8, 10
7	**Limiter la survenue et les conséquences d'incidents de sécurité du SI**	
7.1	**Vérifier le niveau de sécurité des moyens informatiques**	
7.1.1	Procéder à un contrôle régulier de la bonne mise en œuvre des règles de la PSSI	Obj. 10, 21, 24, 33, 34
7.1.2	Procéder à un audit régulier des vulnérabilités du SI	Obj. 34
7.1.3	Assurer un suivi de la disponibilité des ressources informatiques	Obj. 34
7.2	**Conserver les traces informatiques**	
7.2.1	Tracer spécifiquement les actions réalisées sur les données de santé à caractère personnel et sur les autres données sensibles	Obj. 22
7.2.2	Tracer les évènements informatiques	Obj. 20, 21, 22, 23, 24
7.3	**Faire face à un incident de sécurité du SI**	
7.3.1	Anticiper la survenue d'un incident de sécurité	Obj. 32

Thème	Intitulé du thème, sous-thème ou exigence de la PSSI	Objectifs de sécurité PSSIE – Version 1.0 (voir [Réf. n°10])
7.3.2	Détecter un incident de sécurité	Obj. 16, 22
7.3.3	Prendre des mesures pour gérer les incidents de sécurité	
7.4	**Sauvegarder les données**	
7.4.1	Organisation et Plan de sauvegarde	
7.4.2	Règles techniques pour la sauvegarde des serveurs	Obj. 25
7.4.3	Règles techniques pour la sauvegarde des postes de travail	Obj. 25
7.4.4	Règles techniques générales pour la sauvegarde	Obj. 33
7.4.5	Règles relatives à la restauration et au contrôle des sauvegardes	
7.4.6	Règles relatives aux contrats d'externalisation des sauvegardes	
7.5	**Mettre en place un Plan de Continuité Informatique**	
7.5.1	Définir l'organisation nécessaire au Plan de Continuité Informatique	Obj. 33
7.5.2	Elaborer le Plan de Continuité Informatique	Obj. 33
7.5.3	Tester le Plan de Continuité Informatique	Obj. 33

Correspondance entre thématiques PSSI et articles ISO27002

Thématique PSSI	Articles NF ISO/CEI 27002 – janvier 2014 (ISO27002:2013)
T1 - Répondre aux obligations légales	18 - Conformité
T2 - Promouvoir et organiser la sécurité	5 - Politiques de sécurité de l'information
	6 - Organisation de la sécurité de l'information
	7 - La sécurité des ressources humaines
T3 - Assurer la sécurité physique des équipements informatiques du SI	11 - Sécurité physique et environnementale
T4 - Protéger les infrastructures informatiques	8 - Gestion des actifs
	12 - Sécurité liée à l'exploitation
	13 - Sécurité des communications
T5 - Maîtriser les accès aux informations	9 - Contrôle d'accès
	10 - Cryptographie
T6 - Acquérir des équipements, logiciels et services qui préservent la sécurité du SI	14 - Acquisition, développement et maintenance des systèmes d'information
	15 - Relations avec les fournisseurs
T7 - Limiter la survenue et les conséquences d'incidents de sécurité	16 - Gestion des incidents liés à la sécurité de l'information
	17 - Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

IV. RÉFÉRENCES

Référence n°1 : L'hygiène informatique en entreprise (ANSSI)

Référence n°2 : Guide des professionnels de santé (CNIL)

Référence n°3 : Programme Hôpital Numérique – Boîte à outils pour l'atteinte des prérequis – Fiches pratiques (DGOS)

Référence n°3bis : Programme Hôpital Numérique – Boîte à outils : outil d'autodiagnostic et plan d'actions associé (fichier tableur OpenDocument ou Excel) (DGOS)

Référence n°4 : Guide pratique pour la sécurité SI en établissement de santé – Fiches pratiques (DGOS)

Référence n°5 : Recommandations de sécurité relatives aux mots de passe (ANSSI)

Référence n°6 : Référentiels et guides pratique du corpus documentaire PGSSI-S

https://esante.gouv.fr/securite/politique-generale-de-securite-des-systemes-d-information-de-sante

https://esante.gouv.fr/securite/pgssi-s/espace-de-publication

Référence n°6.1 : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée (voir Réf. n°6)

Référence n°6.1bis : Annexe au canevas de PSSI pour les structures des secteurs sanitaire et médico-social : Couverture des règles de la PSSIE par les règles du canevas de PSSI (PGSSI-S) (voir Réf. n°6)

Référence n°6.2 : Modèle de charte d'accès et d'usage du système d'information (voir Réf. n°6)

Référence n°6.3 : Modèle de charte sécurité pour les personnels IT (voir Réf. n°6)

Référence n°6.4 : Guide pratique « Plan de Continuité Informatique - Principes de base » (voir Réf. n°6)

Référence n°6.5 : Guide Pratique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé » (voir Réf. n°6)

Référence n°6.6 : Guide Pratique « Règles pour les dispositifs connectés d'un Système d'Information de Santé » (voir Réf. n°6)

Référence n°6.7 : Guide Pratique « Règles pour la mise en place d'un accès web au SIS pour des tiers » (voir Réf. n°6)

Référence n°6.8 : Guide pratique spécifique pour la mise en place d'un accès Wifi (voir Réf. n°6)

Référence n°6.9 : Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé (voir Réf. n°6)

Référence n°6.10 : Guide pratique « Règles de sauvegarde des Systèmes d'Information de Santé » (voir Réf. n°6)

Référence n°6.11 : Référentiel d'identification des acteurs sanitaires et médico-sociaux (voir Réf. n°6)

Référence n°6.12 : Référentiel d'authentification des acteurs de santé (voir Réf. n°6)

Référence n°7 : Guide de l'externalisation « Externalisation et sécurité des systèmes d'information : maitriser les risques » (ANSSI)

Référence n°8 : TDBSSI – Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information (ANSSI)

Référence n°9 : Référentiel Général de Sécurité (RGS) (https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/)

Référence n°10 : Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) – Version 1.0 (juillet 2014) (http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/)

Référence n°11 : *NF ISO/CEI 27002:2014-01*

V. ÉVALUATION

Tous les ans

VI. DOCUMENTS ASSOCIÉS

Toutes les règles de sécurité numérique dans la GED, l'Intranet, chartes, …

VII. HISTORIQUE DU DOCUMENT

Evolution du document en janvier 2022 suite à l'audit de certification HDS
Evolution du document en été 2021 avec la mise à jour de l'analyse des risques
Mise à jour en décembre 2020 suite à l'audit de pré-certification HDS
Mise à jour en février 2020
Conversion du document au format GED en août 2019

VIII. RÉDACTION, VALIDATION, APPROBATION

Groupe de travail :

NOMS ET FONCTIONS DES SIGNATAIRES	DATES DE SIGNATURE
Relecture qualité	
Ingénieur qualité, Pôle Efficience, Finances et Qualité	**28/01/2022 12:28:15**
Rédaction	
Sylvain Chambeau, Responsable des Services Numériques du CHU **Yann Delahaye**, RSMSI, Responsable convergence infrastructure GHT SLS **Sébastien Florek**, Directeur des Services Numériques du GHT **Dr Paulo Henriques**, Délégué à la Protection des Données du CHU & GHT SLS **Pascal Tourbier**, Responsable Infrastructure Technique CHU	**31/01/2022 08:38:41, 22/03/2022 13:33:31, 04/04/2022 15:38:27, 12/05/2022 08:41:45, 12/05/2022 05:57:34**
Validation	
Julien Rousselle, Ingénieur Responsable de la Sécurité des Systèmes d'Information CHU & GHT SLS	**12/05/2022 08:44:22**
Approbation	
Directeur qualité, Pôle Efficience, Finances et Qualité	**13/05/2022 11:57:06**