



POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DU CH D'HESDIN

VERSION 2.2

Mai 2024

SOMMAIRE

1.	Préambule : déclaration de la Direction.....	4
2.	Objet de la PSSI	5
3.	Champ d'application.....	5
3.1	Périmètre de la PSSI	5
3.2	Le niveau de criticité des ressources du SI	5
3.3	Le système d'information de l'établissement	6
4.	Contexte	8
4.1	Textes et documents de référence applicables	8
4.2	Enjeux de la sécurité du SI	9
4.3	Objectifs de sécurité.....	10
4.4	Principaux risques liés au SI	11
5.	Mise en oeuvre de la PSSI	14
5.1	Applicabilité de la PSSI	14
5.2	Diffusion de la PSSI.....	14
5.3	Révision de la PSSI.....	14
5.4	Gouvernance de la SSI	14
5.5	Suivi de la SSI	16
6.	Principes de sécurité applicables.....	17
6.1	Thématique 1 : Répondre aux obligations légales	17
6.2	Thématique 2 : Promouvoir et organiser la sécurité.....	17
6.3	Thématique 3 : Assurer la sécurité physique des équipements informatiques du SI... 18	
6.4	Thématique 4 : Protéger les infrastructures informatiques	18
6.5	Thématique 5 : Maîtriser les accès aux informations	19
6.6	Thématique 6 : Acquérir des équipements, logiciels et services	19
6.7	Thématique 7 : Limiter la survenue et les conséquences d'incidents de sécurité.....	20
7.	ANNEXES.....	22
7.1	Annexe 1 - Principaux documents liés à la PSSI.....	22
7.2	Annexe 2 – Les ressources prises en compte dans la PSSI.....	23
7.3	Annexe 3 – Synthèse de la couverture des risques par les principes de la PSSI.....	28
7.4	Annexe 4 – Bonnes pratiques SSI	37
7.5	Annexe 5 – Glossaire	38

REVISIONS				
Rédacteur	Relecteur	Approbateur	Date	Version
Jean-Luc BOULAN	Alexandre LEROUX	Aurélie DANILO	02/04/2015	1.02
Alexandre LEROUX	Jean-Luc BOULAN	Philippe SARRIS	27/04/2017	1.03
Alexandre LEROUX	Jean-Luc BOULAN	Olivier FROMENTIN	15/12/2021	2.01
Alexandre LEROUX	Jean-Luc BOULAN	Thomas JOUSSE	15/05/2024	2.02

Droit de copie et protection des droits de propriété intellectuelle

Conformément à l'article 41 de la loi du 11/03/1957, toute reproduction, citation et/ou présentation intégrale ou partielle, du présent document, élaboré par la Direction du Système d'Information du CHAM-CH d'HESDIN, est strictement interdite sans le consentement préalable du Directeur.

1. PREAMBULE : DECLARATION DE LA DIRECTION

Le Système d'Information qui est déployé au sein de l'établissement remplit des fonctions indispensables à sa gestion quotidienne, en particulier celles à la prise en charge des patients. Sa sécurité doit être assurée à tout moment et en toutes circonstances afin de permettre cette prise en charge.

Par ailleurs, certaines informations qu'il traite sont particulièrement sensibles, comme par exemple les données de santé des patients. Le Système d'Information doit garantir que ces informations restent authentiques et confidentielles. Et 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.

Au regard de ces risques, l'établissement a la responsabilité vis-à-vis des patients, des professionnels et de nos tutelles de garantir un niveau de protection suffisant des données qu'il traite.

Pour relever ce défi, une démarche a été lancée pour identifier les lacunes en matière de Sécurité du Système d'Information - SSI - qui pourraient lui faire subir ces risques, élaborer et mis en œuvre un plan d'actions visant à permettre de maîtriser les risques.

La présente Politique de Sécurité des Systèmes d'Information - PSSI - constitue le cadre unique de référence de l'établissement pour toutes les questions de sécurité de son système 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 responsable de service doit communiquer cette politique et s'assurer que les règles sont respectées au sein de son service.

Thomas JOUSSE

Directeur adjoint en charge du Système d'Information

CHAM-CH HESDIN

2. OBJET DE LA PSSI

La PSSI de l'établissement est un document de référence, validé et appuyé par les Directions dont la Direction Générale, qui doit être pris en compte par l'ensemble des acteurs et utilisateurs du Système d'Information Hospitalier.

Elle explicite les principaux enjeux de la sécurisation du Système d'Information pour l'établissement et détermine les principes qui permettent d'assurer cette sécurisation.

Elle définit également l'organisation nécessaire à sa mise en œuvre et la façon dont elle doit être suivie dans le temps.

Elle découle de l'analyse de risques et les principes de sécurité qu'elle énumère sont pris en compte pour l'élaboration du plan d'actions SSI qui vise prioritairement à réduire les risques liés au Système d'Information.

3. CHAMP D'APPLICATION

3.1 PERIMETRE DE LA PSSI

Le périmètre de la PSSI comprend toutes les ressources du Système d'Information exploitées par l'établissement pour assurer ses activités, dès lors que ces dernières nécessitent le traitement de données à caractère personnel.

L'énumération de ces ressources fait l'objet de l'ANNEXE 2 de la PSSI.

3.2 LE NIVEAU DE CRITICITE DES RESSOURCES DU SI

Le niveau de criticité des ressources du SI prises en compte dans le cadre de la PSSI détermine leurs besoins de sécurité selon les quatre critères suivants :

- La disponibilité : le fait que les ressources soient accessibles au moment prévu pour leurs usages autorisés ;
- L'intégrité : le fait que les ressources ne puissent être modifiées que par les personnels habilités à le faire et qu'à défaut tout changement illégitime puisse être détecté ;
- La confidentialité : le fait que les ressources ne soient accessibles qu'aux utilisateurs habilités à y accéder ;
- L'auditabilité ou l'imputabilité : le fait tracer les actions ont été réalisées au sein du SI (qui a fait quoi et quand) et de conserver ces traces comme preuves exploitables.

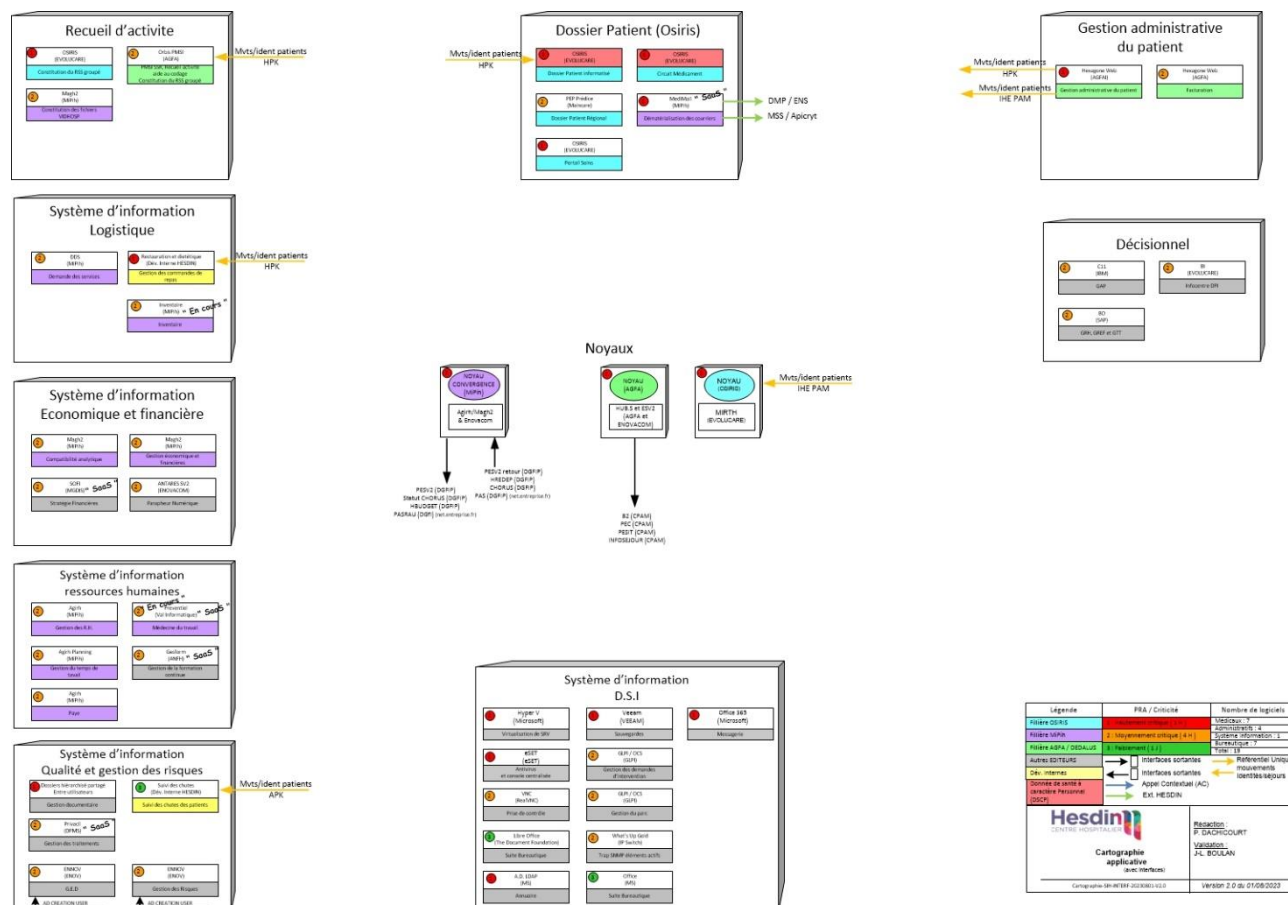
Les besoins de sécurité des ressources du SI prises en compte dans le cadre de la PSSI sont définis dans le cadre de l'analyse de risques consultable auprès de la Direction Générale de l'établissement.

3.3 LE SYSTEME D'INFORMATION DE L'ETABLISSEMENT

3.3.1 Description du SI de l'établissement

Le SI de l'établissement est décrit de façon détaillé dans le Plan de Reprise d'Activité et ses annexes, consultables auprès de la Direction du Système d'Information de l'établissement.

3.3.2 La cartographie applicative



3.3.3 Les applications métiers gérant des données à caractère personnel

Les applications métiers prises en compte dans le cadre de la PSSI sont les suivantes :

Application	Domaine fonctionnel
Hexagone	Gestion administrative du patient, de la facturation, de l'identité et de l'identitovigilance. Référentiel unique d'identités, séjours et mouvements des patients
Osiris	Dossier patient, dossier de soins, dossier SMR, dossier du résident, circuit du médicament, alimentation du DMP/ENS, envoi vers la MSS et gestion des lits et places
Orbis PMSI	PMSI Aide au codage
Suite convergence du MiPih	Gestion des Ressources Humaines Gestion de la Ressource Economique et Financière Gestion du temps de travail
GCR	Gestion des commandes repas
GDC	Gestion et suivi des chutes
Dossiers hiérarchisés	Gestion documentaire
Système d'information de pilotage	C11 sur l'application Hexagone BI sur le DPI Osiris
Gestion des identités	Active Directory
Gestion du parc informatique	GLPI

4. CONTEXTE

4.1 TEXTES ET DOCUMENTS DE REFERENCE APPLICABLES

4.1.1 Cadre légal et réglementaire

Liste des textes légaux et réglementaires applicables :

- CNIL : loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, modifiée ; textes réglementaires d'application, délibérations / recommandations / avis CNIL associés.
- Directive NIS et application au droit national :
 - Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ;
 - Décret no 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;
 - Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret no 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
- Code civil (respect de la vie privée) ;
- Loi n°91-646 du 10 juillet 1991 modifiée sur le secret des correspondances ;
- Loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle ;
- Articles 323-1 et suivants du code pénal ;
- Code la santé publique (loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé consacrant le droit des patients au respect de sa vie privée et au secret des informations le concernant, protection des données personnelles, exploitation et traitement des données médicales, droits d'accès aux données de santé, information des patients et des professionnels de santé, traitements de données à des fins statistiques et épidémiologiques, nécessité d'un agrément des hébergeurs de données de santé, obligation de recourir à la carte de professionnel de santé ou à un dispositif équivalent, identifiant national de santé : INS) ;
- Code de la sécurité sociale (droits des assurés, NIR, remboursement des soins, Carte Vitale) ;
- Code de déontologie professionnelle ;
- Code de la propriété intellectuelle (protection des logiciels, des bases de données) ;
- Loi relative à la fraude informatique (loi Godfrain) ;
- Loi pour la Confiance dans l'Economie Numérique (LCEN) ;
- Les instructions et recommandations interministérielles provenant de la Direction Générale de l'offre de soins (DGOS) ;
- RGPD : Le **Règlement Général sur la Protection des Données**, officiellement appelé règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

4.1.2 Autres textes de référence

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 -, ANS : principes fondateurs et corpus documentaire associé (PSSI) ;
- Politique de Sécurité des Systèmes d'Information de l'Etat -PSSIE -, version 1.0 (circulaire du Premier ministre n° 5725/SG du 17 juillet 2014) ;
- Référentiel Général de Sécurité (RGS), version 2.0 (arrêté du 13 juin 2014) ;
- Norme ISO 27799 « Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002 ».

4.2 ENJEUX DE LA SECURITE DU SI

L'informatisation du dossier patient et de tous les processus de production de soins, permet d'améliorer la sécurité et la qualité des soins au sein de l'établissement. Elle exige de fait que le système d'information puisse fonctionner avec un niveau de disponibilité élevé, et conserver les données dans le temps tout en garantissant leur intégrité et leur confidentialité.

Dans le même temps le système d'information doit fréquemment évoluer pour répondre à de nouveaux besoins en matière de :

- Connectivité : pour l'interfaçage des différentes applications métiers, pour l'intégration des équipements biomédicaux et l'exploitation des informations qu'ils produisent, pour répondre aux demandes d'accès au système d'information qui se diversifient avec l'usage de terminaux « mobiles », etc. ;
- Ouverture : pour favoriser la coordination des soins avec les autres acteurs de santé et permettre d'améliorer la prise en charge des patients tout au long de leurs parcours de soins : échange d'information médicale par messagerie sécurisée, partage de documents médicaux avec le DMP, coopération avec la médecine de ville ou dans le cadre de réseaux de santé, développement de la télémédecine et de la télé imagerie, etc. ;
- Accessibilité : pour permettre aux patients d'accéder plus facilement à leurs dossiers et d'être ainsi pleinement acteurs de leurs parcours de soins (portail patients, etc.).

Toutefois ceci a aussi pour effet 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 gérés par le système d'information.

Dès lors, la sécurité du Système d'Information est une condition indispensable pour garantir une bonne prise en charge des patients et une gestion intègre de l'établissement.

Elle doit donc être maîtrisée tout au long du cycle de vie du Système d'Information, prendre en compte l'évolution des facteurs, tant qu'internes, qu'externes, qui sont susceptibles de l'impacter, et garantir la disponibilité, l'intégrité et la confidentialité des services qu'il offre aux professionnels et des données qu'il exploite.

La sécurité du Système d'Information doit s'inscrire dans une démarche « qualité » et de maîtrise globale des risques, en s'attachant à obtenir l'adhésion des utilisateurs.

4.3 OBJECTIFS DE SECURITE

Afin de répondre aux enjeux de la sécurité du SI, la Direction Générale de l'établissement définit les objectifs de sécurité suivants :

- Contribuer à la qualité et la sécurité de la prise en charge des patients ;
- Protéger les données de santé à caractère personnel et plus généralement le patrimoine informationnel de l'établissement ;
- Assurer la disponibilité du SI, en particulier celle des applications métiers, des services informatiques et des dispositifs médicaux pilotés par le SI, qui participent à la prise en charge des patients ;
- Lutter contre les risques liés à l'usage des moyens informatiques ;
- Limiter l'accès au SI et aux données, ainsi que leur usage, aux seules personnes qui disposent des habilitations nécessaires. Les habilitations qui sont confiées aux utilisateurs du SI sont strictement limitées aux seules dont ils ont besoin pour réaliser leurs missions (principe du moindre privilège) ;
- Protéger les échanges électroniques en interne et vis-à-vis de l'extérieur, proportionnellement à la criticité des informations échangées ;
- Imposer la prise en compte de la sécurité dans le cadre des prestations réalisées par des tiers (prestataires informatiques, éditeurs de logiciels, fournisseurs, etc.) et des produits (matériels et logiciels) qu'ils livrent ;
- Sensibiliser le personnel de l'établissement aux questions de sécurité vis-à-vis de l'usage des outils informatiques, des services applicatifs, et des données qu'ils traitent ;
- Assurer la traçabilité des actions menées au sein du SI et la conservation de ces traces (techniques et fonctionnelles) comme preuves exploitables ;
- Favoriser le développement de la coopération entre professionnels de santé en instaurant un climat de confiance ;
- Contribuer à la stratégie et à l'image de marque de l'établissement ;
- Maîtriser les risques et être complémentaire aux démarches de qualité et de gestion des risques, mettre en œuvre des bonnes pratiques dans le cadre d'une démarche d'amélioration continue ;
- Être en conformité avec le cadre législatif et réglementaire ainsi que l'état de l'art.

4.4 PRINCIPAUX RISQUES LIES AU SI

4.4.1 Méthode d'analyse de risques

La PSSI découle de l'analyse de risques liés au SI de l'établissement.

Cette analyse de risques a été réalisée sur un périmètre identique à celui de la PSSI, à l'aide de la méthode EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité - préconisée par l'Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI -, et par l'Agence du Numérique en Santé - ANS : ex ASIP Santé -.

Le résultat de l'analyse de risques de l'établissement est consultable auprès de la Direction du Système d'Information de l'établissement.

4.4.2 Origines des risques prise en compte

La PSSI ne tient compte que des risques dont l'origine peut être :

- Une catastrophe naturelle ou un accident industriel d'ampleur locale ;
- Une défaillance technique ;
- Une erreur ou un acte de malveillance commis par :
 - Le personnel interne ;
 - Les éditeurs, les fournisseurs voire leurs sous-traitants ;
 - Les usagers et les visiteurs ;
 - Les délinquants ou criminels potentiellement auteurs de vols ou de vandalisme ;
 - Les « cybercriminels » ne visant pas spécifiquement la structure.

La PSSI ne prend pas en considération certaines sources de menaces particulières, car les scénarios par lesquels elles pourraient exploiter les vulnérabilités du SI sont très peu vraisemblables dans le contexte de l'établissement. Par ailleurs les mesures de protection pour y faire face impliqueraient des coûts incompatibles avec son activité.

Les sources de menaces non prises en compte sont :

- Les menaces d'origine étatique (quel que soit le pays) ;
- Les « cybercriminels » qui viseraient spécifiquement la structure et disposeraient des moyens nécessaires pour ce faire.

La PSSI ne considère pas non plus les atteintes de type « espionnage industriel », la structure ne pratiquant pas d'activité de recherche dans des secteurs jugés fortement concurrentiels.

4.4.3 Evènements redoutés et risques

L'analyse de risque de l'établissement a révélé que les sources de menaces prises en compte sont effectivement en mesure d'exploiter les vulnérabilités des biens supports énumérés au paragraphe 3.1 de la PSSI, avec pour effet, selon un certain nombre de scénarios envisageables, la survenue éventuelle des évènements redoutés préalablement déterminés.

Le tableau ci-dessous dresse la liste des évènements redoutés par l'établissement et les conséquences, ou atteintes, qu'ils peuvent occasionner sur les fonctions du SI et les données qu'il exploite. Les différents types d'atteinte déterminent les risques auxquels est exposé l'établissement et les impacts qu'ils peuvent provoquer.

Evènements Redoutés	Risque	Atteintes	
Accès aux données de santé à caractère personnel d'un usager par un tiers non autorisé constituant une atteinte à la vie privée et/ou au secret médical	R_SSI_C1	Visualisation	Des données sont vues par des personnes qui n'ont pas à les connaître, sans que celles-ci ne les exploitent.
	R_SSI_C2	Stockage	Des données sont copiées et sauvegardées illégitimement à un autre endroit, sans être davantage exploitées.
	R_SSI_C3	Rediffusion	Des données sont diffusées plus que nécessaire et échappent à la maîtrise des personnes concernées.
	R_SSI_C4	Exploitation	Des données sont exploitées à d'autres fins que celles prévues et/ou de manière injuste ou corrélées avec d'autres informations relatives aux personnes concernées.
Altération de fonctions (application médicale, dispositif connecté, ...) ou d'informations (données de santé à caractère personnel ou personnelles d'un usager) pouvant entraîner une désorganisation du service, un impact d'image négatif auprès des usagers ou un risque patient	R_SSI_I5	Dysfonctionnement	Des fonctions du SI sont altérées ou des données sont modifiées en des données valides ou invalides qui ne sont plus utilisées de manière correcte, leurs traitements pouvant engendrer des erreurs, des dysfonctionnements, ou ne plus fournir le service attendu.
	R_SSI_I6	Blocage	Des fonctions du SI sont altérées ou des données sont modifiées en d'autres données valides, de telle sorte qu'elles ne peuvent plus être exploitées.
Indisponibilité de fonctions (application médicale, dispositif connecté, ...) ou d'informations (données de santé à caractère personnel ou données personnelles d'un usager) pouvant entraîner une désorganisation du service, un impact d'image négatif auprès des usagers ou un risque patient	R_SSI_D7	Dysfonctionnement	Des fonctions sont indisponibles ou des données sont manquantes à des traitements, ce qui génère des erreurs, des dysfonctionnements, ou fournit un service différent de celui attendu.
	R_SSI_D8	Blocage	Des fonctions sont indisponibles ou des données sont manquantes à des traitements qui ne peuvent plus du tout fournir le service attendu.
Modification de données d'imputabilité pouvant notamment augmenter le risque juridique pour la structure en cas de contentieux	R_SSI_A9	Dysfonctionnement	Les données d'imputabilité sont modifiées, leur traitement ne permettant ni de déterminer précisément l'origine d'un incident de sécurité, ni de définir complètement les mesures

			appropriées pour en limiter les conséquences ou en corriger les causes.
	R_SSI_A10	Blocage	Les données d'imputabilité sont modifiées de telle sorte que leur traitement engendre une analyse erronée d'un incident de sécurité, ce qui conduit à la mise en place de mesures inefficaces voire inappropriées.

Le niveau de chaque risque est déterminé selon la matrice ci-dessous, en combinant le niveau de gravité de son impact avec le niveau de vraisemblance le plus élevé des scénarios de menace conduisant à la survenue de l'évènement redouté correspondant.

		Vraisemblance			
		Exceptionnel	Peu probable	Plausible	Quasi certain
Gravité	Mineure	Limité	Limité	Limité	Limité
	Significative	Limité	Modéré	Modéré	Modéré
	Importante	Limité	Modéré	Modéré	Fort
	Critique	Modéré	Fort	Fort	Fort

Les échelles qui permettent d'évaluer le niveau de vraisemblance des scénarios de menaces et celui de gravité des impacts des risques sont définies dans l'analyse de risques de l'établissement.

4.4.4 Stratégie de traitement des risques

Les mesures mises en œuvre dans le cadre de la PSSI visent à réduire l'ensemble des risques liés au SI.

L'application de ces mesures permet de ramener les risques résiduels à un niveau « Limité », que ce soit par la réduction des cas de réalisation des scénarios de menace, ou par la limitation de leurs impacts sur l'établissement.

Le poids de ces risques résiduels est en partie partagé avec des organismes d'assurance.

Cette stratégie de réduction des risques se concrétise par des mesures organisationnelles et techniques, mises en œuvre dans le cadre d'un plan d'actions SSI, priorisé selon l'échelle ci-dessous :

Echelle d'objectif de traitement du risque	
Risque	Critères de gestion des risques (Règles de définition des priorités pour réaliser les actions)
Limité	Risques non critiques. Situations à risque acceptables en l'état. Des mesures peuvent être mises en œuvre, ou consolidées, afin de maintenir le risque à ce niveau
Modéré	Risques à surveiller. Situation à risque acceptables en l'état à condition que des actions soient menées pour mieux les identifier et les surveiller, ou que des mesures adaptées soient programmées à moyen terme pour les réduire
Fort	Risques à traiter en priorité. Situations à risque non acceptables en l'état, nécessitant sans délai des actions d'analyse complémentaire, si nécessaire, et surtout de traitement pour réduire le risque au moins au niveau inférieur.

5. MISE EN OEUVRE DE LA PSSI

5.1 APPLICABILITE DE LA PSSI

La PSSI est formellement approuvée par la Direction Générale, elle est de fait applicable en l'état au sein de l'établissement.

5.2 DIFFUSION DE LA PSSI

La PSSI est portée à la connaissance de l'ensemble des acteurs et des utilisateurs du SI.

5.3 REVISION DE LA PSSI

La PSSI fait l'objet d'une mise à jour à minima tous les 3 ans.

La révision de la PSSI peut également être exigée à tout moment pour les raisons suivantes :

- Une évolution majeure du contexte de l'établissement et/ou de son SI ;
- Une révision des objectifs de sécurité ;
- L'identification de nouvelles menaces ;
- Les résultats d'un audit ;
- L'évolution du cadre législatif ou réglementaire ;
- La demande d'une autorité.

Une nouvelle analyse de risques doit être réalisée préalablement à chaque mise à jour de la PSSI, et cette dernière doit entraîner la revue du plan d'actions SSI, ainsi que celle des procédures opérationnelles et de la « Charte Utilisateurs », pour une mise en cohérence des documents si cela s'avère nécessaire.

5.4 GOUVERNANCE DE LA SSI

5.4.1 La Direction de l'établissement

La Direction Générale de l'établissement est responsable de la mise en œuvre de la PSSI. Elle a pour rôle :

- De fixer les orientations de l'établissement en matière de sécurité du SI ;

- D'inscrire le pilotage de la Sécurité du SI (SSI) dans le cadre d'une démarche d'amélioration continue, visant prioritairement la réduction des risques identifiés ;
- De définir et d'attribuer les moyens nécessaires à la mise en œuvre de la PSSI.

Elle désigne le **Correspondant local de la Sécurité du SI - CSSI** - sous couvert du **Responsable de la Sécurité du SI - RSSI** - de GHT. Ses missions sont précisées dans une fiche de poste. Il est assisté dans sa mission par un **Comité de Pilotage de la SSI - COPIL SSI** -.

5.4.2 Le CSSI

Le CSSI est désigné par la Direction Générale. Il est placé sous son autorité en ce qui concerne les missions qui lui incombent. Les missions et les activités qui lui sont confiées sont les suivantes :

- Définition et mise en œuvre de la PSSI ;
- Diagnostic et analyse des risques de la sécurité des systèmes d'information ;
- Choix des mesures de sécurité et plan de mise en œuvre ;
- Sensibilisation, formation et conseil sur les enjeux de la sécurité des SI ;
- Audit et contrôle de l'application des règles de la PSSI ;
- Veille technologique et prospective.

5.4.3 Le Comité de Pilotage SSI (COPIL SSI)

Le Comité de Pilotage de la SSI a pour rôle de décider, d'orienter, de contrôler, et de valider l'ensemble des actions relatives à la SSI à entreprendre. C'est également un lieu de partage de l'information relative à la SSI.

Il donne son avis sur les orientations relatives à la SSI, notamment sur le plan d'action SSI, le rapport annuel SSI, etc.

Il est placé sous la responsabilité de la Direction Générale de l'établissement et il est organisé et animé par le CSSI sous couvert du RSSI de GHT.

L'ensemble des directions et métiers de l'établissement sont présents ou représentés.

Le comité se réunit au moins une fois par semestre.

5.4.4 Les responsables opérationnels

Les responsables opérationnels - responsables de services, etc. - ont le devoir, dans le cadre de leurs missions et de leurs périmètres d'intervention, de promouvoir et de faire respecter les principes de sécurité de la PSSI.

5.4.5 Les acteurs et les utilisateurs du SI

Les acteurs sont les personnes qui, au sein de l'établissement, assurent le déploiement, l'exploitation et la maintenance du SI, ou y contribuent.

Les utilisateurs du SI sont les personnes qui, au sein de l'établissement, bénéficient des fonctions du SI pour réaliser les missions qui leur sont confiées.

Les acteurs et les utilisateurs du SI sont responsables de leurs actes et, à ce titre, ils sont informés et sensibilisés à la sécurité de l'information. En outre, ils doivent :

- Respecter les obligations légales et réglementaires ;
- Respecter les règles et procédures de sécurité en vigueur, issues des principes de sécurité de la PSSI ;
- Informer leur responsable hiérarchique et/ou le CSSI et/ou le RSSI des anomalies ou incidents de sécurité qu'ils constatent.

5.4.6 Les prestataires externes

Les prestataires externes qui accèdent au SI, ou à des informations sensibles concernant le SI et sa sécurité, sont soumis aux mêmes règles que celles qui s'imposent en la matière aux personnels internes.

Les chartes passées entre l'établissement et ces prestataires externes comportent des clauses précisant les obligations et responsabilités de ces derniers en matière de sécurité du SI.

5.4.7 Le délégué à la protection des données personnelles (DPDP/ DPO)

L'établissement a désigné un **Délégué à la Protection Des Données - DPDP - ou Data Protection Officer - DPO -**, conformément à la réglementation. Il s'agit du DPO de GHT qui est un agent de l'établissement support. Ce dernier peut s'appuyer sur le **Référent Informatique et Liberté - RIL -** de l'établissement.

Le DPO contribue, dans le cadre de ses missions, à la définition, la mise en œuvre de la politique de confidentialité des données personnelles et contrôle son application.

Le DPO contrôle le respect de la réglementation, il est conseiller de la Direction et des responsables de traitement, il est également point de contact vis-à-vis de la CNIL.

Le DPO collabore avec le CSSI de l'établissement et le RSSI pour la protection des données personnelles.

5.5 SUIVI DE LA SSI

5.5.1 Contrôles internes SSI

Les objectifs relatifs aux contrôles internes sont définis par le comité de pilotage SSI et les actions correspondantes sont formalisées dans le plan d'actions SSI.

Les contrôles portent principalement sur les aspects suivants :

- L'application des règles et des procédures de sécurité ;
- L'efficacité des règles des procédures de sécurité ;
- Le pilotage de la SSI.

Le CSSI/RSSI a la responsabilité du contrôle interne relatif à la SSI.

Les résultats des contrôles internes peuvent donner lieu à des propositions d'évolutions de la PSSI.

5.5.2 Audits SSI

Des audits de sécurité (organisationnels, techniques) sont menés sous la responsabilité du RSSI. Ils ont pour but de valider l'efficacité des mesures, des dispositifs et procédures de sécurité et de leur niveau de résistance (le cas échéant).

Ils sont menés soit par des expertises internes, soit par des expertises externes sur les périmètres déterminés par le comité de pilotage.

Les résultats des audits peuvent donner lieu, à une nouvelle analyse de risques et/ou à des propositions d'évolutions de la PSSI.

5.5.3 Suivi et bilan de la SSI

La mise en œuvre de la PSSI s'inscrit dans le cadre d'une démarche d'amélioration continue et de contrôle qualité.

Le CSSI/RSSI établit chaque année un bilan de la mise en œuvre de la SSI au sein de l'établissement.

6. PRINCIPES DE SECURITE APPLICABLES

Ce chapitre énumère les principes de sécurité applicables pour atteindre les objectifs de sécurité définis par la Direction Générale.

Ces principes sont déclinés 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.

Chaque thématique comporte une ou plusieurs sous-thématiques pour lesquelles la PGSSI-S de l'ANS énonce un ensemble d'exigences et de règles de sécurité également applicables.

Ces dernières ne sont pas détaillées dans la PSSI mais elles sont néanmoins prises en compte pour l'état des lieux SSI qui est réalisé dans le cadre de l'analyse de risques, ainsi que pour l'élaboration du plan d'actions SSI.

La synthèse de la couverture des risques par les principes de sécurité énumérés ci-après est présentée en ANNEXE 3 de la PSSI.

6.1 THEMATIQUE 1 : REPONDRE AUX OBLIGATIONS LEGALES

1.1	Respecter les principes de la protection des données à caractère personnel
1.1.1	Documenter la conformité au RGPD et à la loi Informatique et Liberté
1.1.2	Sensibiliser le personnel aux enjeux concernant les données à caractère personnel
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	Informar l'utilisateur 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
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
1.4	Veille réglementaire
1.4.1	Assurer une veille réglementaire des dispositions applicables à la structure en matière de SSI

6.2 THEMATIQUE 2 : PROMOUVOIR ET ORGANISER LA SECURITE

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

2.1.2	Formaliser les remontées d'informations sur la sécurité à la direction
2.1.3	Piloter la SSI au sein de l'établissement
2.2	Faire connaître les principes essentiels de sécurité informatique
2.2.1	Sensibiliser, former et responsabiliser le personnel
2.2.2	Décliner les règles du guide dans les procédures opérationnelles

6.3 THEMATIQUE 3 : ASSURER LA SECURITE PHYSIQUE DES EQUIPEMENTS INFORMATIQUES DU SI

3.1	Maîtriser l'accès aux équipements du SI qui sont nécessaires à l'activité de la structure
3.1.1	Assurer la protection physique des équipements informatiques d'infrastructure du SI, qui contiennent des données de santé à caractère personnel
3.1.2	Assurer la protection physique des postes de travail, qui contiennent des données de santé à caractère personnel
3.1.3	Assurer la protection physique des équipements amovibles (disque dur externe, clé USB, CD, DVD) qui contiennent des données de santé à caractère personnel
3.1.4	Assurer la destruction de données lors du transfert (cession, don...) de matériels informatiques

6.4 THEMATIQUE 4 : PROTEGER LES INFRASTRUCTURES INFORMATIQUES

4.1	Maîtrise le parc informatique
4.1.1	Identifier physiquement chaque équipement informatique ou dispositif médical connecté détenu par la structure
4.1.2	Identifier les composants logiciels du SI
4.1.3	Identifier les services d'infrastructure du SI
4.1.4	Vérifier régulièrement la complétude du recensement et les licences
4.1.5	Documenter le SI
4.2	Gérer le réseau local
4.2.1	Identifier ou authentifier chaque équipement connecté au SI
4.2.2	Cloisonner les réseaux selon les besoins de sécurité
4.3	Gérer la connexion Internet
4.3.1	Sécuriser la connexion Internet
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 Wi-Fi "professionnel"

4.4.2	Assurer l'exploitation d'un point d'accès Wi-Fi "professionnel"
4.4.3	Sécuriser la mise en place d'un point d'accès Wi-Fi "invité"
4.5	Protéger l'accès aux systèmes
4.5.1	Gérer les mots de passe pour qu'ils présentent une robustesse appropriée
4.5.2	Verrouiller les postes de travail
4.5.3	Assurer la protection logique des équipements informatiques
4.5.4	Vérifier l'authenticité des logiciels
4.5.5	Procéder à une mise à niveau régulière des moyens informatiques
4.5.6	Assurer la protection logique des supports informatiques et équipements mobiles qui contiennent des données de santé à caractère personnel

6.5 THEMATIQUE 5 : MAITRISER LES ACCES AUX INFORMATIONS

5.1	Accorder les accès aux informations aux seules personnes dûment autorisées
5.1.1	Formaliser des règles d'accès aux informations
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
5.2.2	Utiliser les dispositifs d'authentification en respectant les consignes de sécurité
5.2.3	Protéger les comptes contre les tentatives d'usurpation d'identité
5.2.4	Protéger les comptes administrateurs techniques par défaut
5.3	Lutter contre les accès non autorisés
5.3.1	Utiliser des moyens garantissant la sécurité des échanges

6.6 THEMATIQUE 6 : ACQUERIR DES EQUIPEMENTS, LOGICIELS ET SERVICES

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
6.1.2	Mettre en œuvre des dispositions techniques de sécurité spécifiques dans le SI
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

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
6.3.2	Vérifier les fonctionnalités de sécurité au regard de la PSSI
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 transfert 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
6.5.2	Valider les nouveaux composants du SI avant leur mise en production
6.5.3	Assurer la formation aux nouveaux composants du SI
6.6	Définir l'objet des prestations et les limites d'engagement dans les relations contractuelles avec des tiers fournisseurs de service
6.6.1	Définir précisément dans le contrat le contenu des prestations confiées au tiers fournisseur de service pour répondre aux obligations de sécurité
6.6.2	S'assurer de la capacité de restitution des données de santé à caractère personnel sous une forme réutilisable par la structure
6.6.3	Clauses de sécurité en cas d'externalisation de la destruction des données

6.7 THEMATIQUE 7 : LIMITER LA SURVENUE ET LES CONSEQUENCES D'INCIDENTS DE SECURITE

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
7.1.2	Procéder à un audit régulier des vulnérabilités du SI
7.1.3	Assurer un suivi de la disponibilité des ressources informatiques
7.2	Conserver les traces informatiques
7.2.1	Tracer spécifiquement les actions réalisées sur les données de santé à caractère personnel
7.2.2	Tracer les événements informatiques
7.3	Faire face à un incident de sécurité
7.3.1	Anticiper la survenue d'un incident de sécurité
7.3.2	Détecter un incident de sécurité
7.3.3	Prendre les 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
7.4.3	Règles techniques pour la sauvegarde des postes de travail
7.4.4	Règles techniques générales pour la sauvegarde
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 de fonctionnement du SIS
7.5.1	Définir l'organisation nécessaire au Plan de Continuité de fonctionnement du SIS
7.5.2	Elaborer le Plan de continuité de fonctionnement du SIS
7.5.3	Tester le Plan de continuité de fonctionnement du SIS

7. ANNEXES

7.1 ANNEXE 1 - PRINCIPAUX DOCUMENTS LIES A LA PSSI

La PSSI est complétée par d'autres documents qui constituent ainsi son corpus documentaire : cartographies, inventaires, schémas, procédures et modes opératoires, plan d'action SSI, etc.

Les documents suivants lui sont directement liés :

Document	Référence du document
Etat de lieux et analyse des risques liés au SI	Cartographie-Des-Risques-Informatique-DSI-CHH_20210614.pdf
Le plan d'actions SSI	Plan-D-Actions-SSI_20210302-Suivi-du-PASSI-309-CH-HESDIN.pdf
Procédure de gestion des incidents de sécurité	3 SIN 004 B Procédure de signalement incident grave du système informatique

7.2 ANNEXE 2 – LES RESSOURCES PRISES EN COMPTE DANS LA PSSI

Les tableaux ci-dessous listent les ressources intégrées au périmètre de la PSSI.

7.2.1 Les processus métiers

Processus	Description
Domaine médico-administratif	
Gestion administrative des patients	Annonces d'hospitalisation, préadmissions et admissions - séjours et mouvements - gestion administrative -facturation et échanges avec les tutelles
Gestion des identités des patients	Base patient unique, identité vigilance
Gestion de l'information médicale	Recueil de l'activité, aide au codage, production du PMSI, contrôle qualité
Domaine de la production de soins	
Gestion des dossiers médicaux et paramédicaux des patients	Dossier médical, dossier de soins, dossier du résident
Gestion des prescriptions multimodales	Médicaments, actes, examens
Gestion des activités médico techniques	pharmacie - circuit du médicament -
Domaine des parcours et de la coordination	
Gestion des parcours des patients	Orientation des patients, dossier de coordination et dossier médical personnel

Domaine des fonctions supports	
Gestion des activités logistiques et techniques	Restauration, services hôteliers, téléphonie, brancardage et transport des patients, véhicules professionnels, sécurité des locaux et des personnes
Gestion des équipements médicaux	Equipements médicaux de diagnostic, de traitement et de suivi
Gestion des archives	Archives médicales et administratives
Gestion des ressources du Système d'Information	Mise à disposition, administration et exploitation des ressources, registres des utilisateurs, suivi des pannes et des incidents
Gérer les annuaires	Salariés, professionnels libéraux, prestataires externes, fournisseurs, etc.
Gérer la messagerie professionnelle	Messagerie interne et messagerie sécurisée
Gérer les services internet	Sites internet « grand public »
Gestion des ressources humaines	Gestion administrative du personnel, gestion du temps de travail, paies, formations, carrières, dossiers sociaux, médecine du travail
Gestion de la démarche Qualité	Evènements indésirables, vigilances et enquêtes
Pilotage de l'activité	Statistiques et pilotage médico-économique

7.2.2 Les données

Données	Description
Données à caractère personnel	Toutes les données gérées dans la cadre des activités de l'établissement et dont il est responsable du traitement qui permettent d'identifier directement ou indirectement une personne physique
Données de santé à caractère personnel	Toutes les données gérées dans la cadre des activités de l'établissement et dont il est responsable de traitement : - qui ont trait à la santé physique ou mentale, passée, présente ou future, d'une personne physique (qui révèlent des informations sur l'état de santé de cette personne) ; - qui comportent des indications permettant d'identifier la personne physique directement ou indirectement.

Catégories particulières de données à caractère personnel (autres que les données de santé)	Toutes les données gérées dans la cadre des activités de l'établissement et dont il est responsable de traitement : - qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ou qui concernent la vie sexuelle ou l'orientation sexuelle, ainsi que les données génétiques et les données biométriques, d'une personne physique - qui comportent des indications permettant d'identifier la personne physique directement ou indirectement
Données de référence	Données à caractère général et n'entrant pas dans le cadre des données à caractère personnel (nomenclatures métiers utilisées, bases de connaissance, base de données médicamenteuses, etc.)

7.2.3 Les biens supports

Les matériels	
Les ordinateurs	Matériels informatiques permettant de traiter automatiquement des données et comprenant les organes nécessaires à son fonctionnement autonome, ses interfaces de communication et ses périphériques indispensables, qu'il soit fixe ou mobile. Exemples : serveur, poste de travail, micro-ordinateur portable, assistant personnel, tablette, etc.
Les supports électroniques	Support électronique connectable à un ordinateur ou à un réseau informatique pour le stockage de données numériques. Exemples : CD-ROM, clef USB, cartouche de sauvegarde, disque dur amovible, bande magnétique, carte mémoire, etc.
Les périphériques informatiques	Matériels informatiques optionnels, que l'on doit connecter aux ordinateurs par une interface de communication (ports, connecteurs et adaptateurs), et qui réalise l'entrée et/ou la sortie de données. Exemples : imprimante, scanner, copieur multifonctions, périphérique de sauvegarde amovible, microphone, caméra, etc.
Les logiciels	
Les systèmes d'exploitation	Logiciel d'un ordinateur constituant le socle opérationnel sur lequel vont s'exécuter l'ensemble des autres logiciels (services ou applications). Les principaux éléments du système d'exploitation sont des services de gestion du matériel, les services de gestion des tâches ou des processus ainsi que les services de gestion des droits utilisateurs. Exemples : Microsoft Windows, Linux sous ses différentes distributions, MacOS, etc.
Les systèmes de gestion de bases de données	Ensemble des programmes permettant l'accès, l'ajout, la mise à jour et la recherche au sein d'une base de données. Exemples : Iris, Oracle, SQL Server, etc.

Les intergiciels (middleware)	Logiciels de communication entre les systèmes d'exploitation et les applications, gérant les appels de fonctions de l'application ou de renvoi des résultats. Ils se caractérisent par le fait qu'ils complètent les services des systèmes d'exploitation et qu'ils ne sont pas directement au service des utilisateurs ou des applications. Exemples : EAI (Enterprise Application Integration), ETL (Extract Transform Load)
Les applications métiers standards	Logiciel commercial conçu pour donner aux utilisateurs un accès direct aux services et aux fonctions qu'ils exigent de leur système d'information dans le cadre de leur profession. Exemples : logiciel de gestion administrative des patients, des dossiers patients informatisés, du personnel, etc.
Les progiciels standards	Ce sont des produits complets commercialisés comme tels (plutôt que comme exemplaire unique ou comme développements spécifiques) avec un support, une version et une maintenance. Ils fournissent des services destinés aux utilisateurs et aux applications, mais ne sont pas personnalisés ou spécifiques comme le sont les applications métiers. Exemples : suites bureautiques, logiciels décisionnels, logiciels de messagerie électronique, logiciels d'annuaire, logiciels de serveur web, etc.
Les canaux informatiques (réseaux)	
Le réseau informatique	Vecteur de communications informatiques sous forme numérique. Exemples : réseau filaire, cordon réseau, fibre optique, ondes radio, Wi-Fi, etc.
Le matériel de réseau	Dispositifs intermédiaires ou relais, actifs ou passifs, informatiques, qui transportent et aiguillent des données. Exemples : pont, routeur, hub, firewall, commutateur téléphonique, modem, etc.
Les logiciels des matériels actifs de réseau	Logiciels installés dans les matériels actifs de réseau, indispensables à leur fonctionnement, administration et maintenance. Exemples : firmware, interfaces d'administration, load balancer, etc.
Les logiciels réseau	Progiciels destinés au bon fonctionnement et à la gestion sécurisée du réseau. Exemples : firewall, proxy, logiciels de supervision du réseau, etc.

Les personnes	
Les décideurs	Les décideurs sont les propriétaires des ressources, ainsi que les dirigeants de l'établissement accédant au Système d'Information. Exemple : direction générale
Les professionnels de santé	Personnes internes ou externes exerçant une profession médicale, de la pharmacie ou de la physique médical, ou d'auxiliaires médicaux, et accédant au Système d'Information. Exemples : médecins, infirmiers, assistantes sociales, masseurs-kinésithérapeutes, diététiciens, aides-soignants, etc.
Les personnes déléguées	Personnes agissant sous le contrôle d'un professionnel de santé et à qui ce dernier délègue des droits d'accès au Système d'Information. Exemple : secrétaires médicales
Le personnel administratif	Personnel administratif accédant au Système d'Information. Exemples : personnes en charge de l'accueil des patients, de la prise de rendez-vous, de la facturation, de la gestion des RH, des relations fournisseurs, etc.
Médecin responsable de l'information médicale	Le médecin et les Techniciens du département d'Information Médicale (DIM)
Le personnel informatique et technique	Personnel interne assurant la maintenance, l'exploitation, l'administration technique ou de sécurité des composants du Système d'Information. Exemples : responsables, administrateurs ou techniciens informatiques, personnel en charge de l'entretien et de la maintenance des servitudes essentielles, etc.
Les intervenants externes	Personnel externe assurant la fourniture, la maintenance, l'exploitation, l'administration technique ou de sécurité des matériels, des logiciels et des réseaux, y compris leurs sous-traitants et les personnels mandatés par ceux-ci dans ce cadre. Exemples : prestataires informatiques, éditeurs, prestataires d'hébergement, etc.
Les locaux	
Les locaux sensibles	Tous les emplacements où sont installés les composants matériels du Système d'Information ou les servitudes essentielles. Exemple : les bâtiments, les salles informatiques, les locaux techniques, les bureaux, etc.
Les servitudes essentielles	Tous les services nécessaires au fonctionnement des composants matériels du Système d'Information, et à la sécurité des locaux. Exemples : réseau / alimentation électrique, climatisation, dispositifs de de détection et d'extinction contre l'incendie, dispositifs de de détection d'inondation, alarme, vidéosurveillance, gestion des accès aux locaux, etc.
L'organisme	
Les organisations	La Direction Générale, les services, les tutelles, les organismes externes, les fournisseurs et les entreprises prestataires de services

7.3 ANNEXE 3 – SYNTHÈSE DE LA COUVERTURE DES RISQUES PAR LES PRINCIPES DE LA PSSI

PRINCIPES DE SECURITE DE LA PSSI		R_SSI_C1	R_SSI_C2	R_SSI_C3	R_SSI_C4	R_SSI_I5	R_SSI_I6	R_SSI_D7	R_SSI_D8	R_SSI_A9	R_SSI_A10
1	Répondre aux obligations légales										
1.1	Respecter les principes de la protection des données à caractère personnel										
1.1.1	Documenter la conformité au RGPD et à la loi Informatique et Libertés	X	X	X	X	X	X				
1.1.2	Sensibiliser le personnel aux enjeux concernant les données à caractère personnel	X	X	X	X	X	X	X	X		
1.1.3	Respecter les droits des personnes	X	X	X	X	X	X	X	X		
1.2	Respecter les règles d'échange et de partage de DSCP										
1.2.1	Informier l'utilisateur et recueillir son consentement	X	X	X	X						
1.2.2	Limiter l'accès aux DSCP aux personnes participant à la prise en charge	X	X	X	X	X	X				
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	X	X	X	X						

4.2	Gérer le réseau local										
4.2.1	Identifier ou authentifier chaque équipement connecté au SI	X	X	X	X		X			X	X
4.2.2	Cloisonner les réseaux selon les besoins de sécurité	X	X	X	X		X			X	X
4.3	Gérer la connexion Internet										
4.3.1	Sécuriser la connexion Internet	X	X	X	X		X			X	X
4.3.2	Limiter les accès Internet en conformité avec la Charte d'Utilisation des Ressources Informatiques	X	X	X	X		X			X	X
4.3.3	Conserver une trace des connexions Internet	X	X	X	X		X			X	X
4.4	Gérer les connexions sans fil										
4.4.1	Sécuriser la mise en place d'un point d'accès Wi-Fi	X	X	X	X		X			X	X
4.4.2	Assurer l'exploitation d'un point d'accès Wi-Fi					X		X	X		
4.4.3	Sécuriser la mise en place d'un point d'accès Wi-Fi "invité"	X	X	X	X		X				
4.5	Protéger l'accès aux systèmes (postes de travail, serveurs, équipements réseau, dispositifs connectés...)										
4.5.1	Gérer les mots de passe pour qu'ils présentent une robustesse appropriée	X	X	X	X		X				

4.5.2	Verrouiller les postes de travail	X	X	X	X		X				
4.5.3	Assurer la protection logique des équipements informatiques							X	X	X	X
4.5.4	Vérifier l'authenticité des logiciels					X	X	X	X	X	X
4.5.5	Procéder à une mise à niveau régulière des moyens informatiques							X	X		
4.5.6	Assurer la protection logique des supports informatiques et équipements mobiles (smartphone, tablettes, ...) qui contiennent des données sensibles	X	X	X	X		X			X	X
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	X	X	X	X		X			X	X
5.1.2	Gérer les accès aux informations	X	X	X	X		X			X	X
5.2	Adopter les bonnes pratiques en matière d'authentification des utilisateurs										
5.2.2	Utiliser les dispositifs d'authentification en respectant les consignes de sécurité	X	X	X	X		X			X	X
5.2.3	Protéger les comptes contre les tentatives d'usurpation d'identité	X	X	X	X		X			X	X
5.2.4	Protéger les comptes des services et les comptes administrateurs techniques par défaut	X	X	X	X		X			X	X

7.1.2	Procéder à un audit régulier des vulnérabilités du SI	X	X	X	X	X	X	X	X	X	X
7.1.3	Assurer un suivi de la disponibilité des ressources informatiques					X		X	X		
7.2	Conserver les traces informatiques										
7.2.1	Tracer spécifiquement les actions réalisées sur les DSCP et sur les autres données sensibles	X	X	X	X	X	X	X	X	X	X
7.2.2	Tracer les évènements informatiques	X	X	X	X	X	X	X	X	X	X
7.3	Faire face à un incident de sécurité										
7.3.1	Anticiper la survenue d'un incident de sécurité	X	X	X	X	X	X	X	X	X	X
7.3.2	Détecter un incident de sécurité	X	X	X	X	X	X	X	X	X	X
7.3.3	Prendre les mesures pour gérer les incidents de sécurité	X	X	X	X	X	X	X	X	X	X
7.4	Sauvegarder les données										
7.4.1	Organisation et Plan de sauvegarde					X	X	X	X		
7.4.2	Règles techniques pour la sauvegarde des serveurs					X	X	X	X		
7.4.3	Règles techniques pour la sauvegarde des postes de travail					X	X	X	X		

7.4.4	Règles techniques générales pour la sauvegarde					X	X	X	X		
7.4.5	Règles relatives à la restauration et au contrôle des sauvegardes					X	X	X	X		
7.4.6	Règles relatives aux contrats d’externalisation des sauvegardes					X	X	X	X	X	X
7.5	Mettre en place un Plan de Continuité de fonctionnement du SIS										
7.5.1	Définir l’organisation nécessaire au Plan de Continuité de fonctionnement du SIS							X	X		
7.5.2	Elaborer le Plan de Continuité de fonctionnement du SIS							X	X		
7.5.3	Tester le Plan de Continuité de fonctionnement du SIS							X	X		

7.4 ANNEXE 4 – BONNES PRATIQUES SSI

Dans le cadre de la démarche d'amélioration continue mise en œuvre au sein de l'établissement et au titre de la veille organisée par le CSSI/RSSI, de nombreuses bonnes pratiques SSI sont à analyser et appliquer (dans la mesure où l'établissement le décide).

L'étude et la mise en œuvre de ces bonnes pratiques peut utilement précéder la mise en œuvre d'une démarche SSI plus formalisée basée sur une méthode d'analyse de risque telle qu'EBIOS.

Les principales bonnes pratiques disponibles (à date) sont classées par émetteur.

7.4.1 ANSSI

7.4.1.1. Recommandations & guides

Lien : <https://www.ssi.gouv.fr/administration/bonnes-pratiques/>

7.4.1.2. Guide d'hygiène informatique

Document destiné aux PME (tout secteur d'activité), il donne les principales règles pour l'application de règles de base.

Lien : <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

7.4.2 Agence du Numérique en Santé (ex ASIP Santé)

L'ANS met à disposition dans le cadre de la PGSSI-S - Politique Générale de Sécurité des SI de Santé - de nombreux documents : référentiels (opposables à terme), guides de bonnes pratiques, etc.

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

7.4.3 Ministère de la Santé

Cybersécurité.

Liens :

<https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/memento-de-cybersecurite>

[https://solidarites-sante.gouv.fr/IMG/pdf/guide - introduction a la securite du systeme d information - dgos - 091213.pdf](https://solidarites-sante.gouv.fr/IMG/pdf/guide_-_introduction_a_la_securite_du_systeme_d_information_-_dgos_-_091213.pdf)

https://solidarites-sante.gouv.fr/IMG/pdf/dgos_memento_ssi_131117.pdf

INSTRUCTION N°DGOS/MSIOS/2013/384 du 19 novembre 2013 relative à la publication du guide pour les directeurs des établissements de santé : introduction à la sécurité des Systèmes d'Information en établissements de santé.

Lien : http://circulaires.legifrance.gouv.fr/pdf/2013/11/cir_37655.pdf

INSTRUCTION N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés.

Lien : http://circulaire.legifrance.gouv.fr/pdf/2016/11/cir_41533.pdf

INSTRUCTION N° DGOS/PF5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme HOP'EN.

Lien : http://circulaires.legifrance.gouv.fr/pdf/2019/02/cir_44396.pdf

7.5 ANNEXE 5 – GLOSSAIRE

Sigle / Acronyme	Signification
ANAP	Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANS	Agence du Numérique en Santé (ex ASIP Santé)
CNIL	Commission Nationale de l'Informatique et des Libertés
COPIL-SSI	COmité de PILOTage de la Sécurité du Système d'Information
CSSI	Correspondant de la Sécurité du Système d'Information
DGOS	Direction Générale de l'Offre de Soins
DIM	Département d'Information Médicale
DMP	Dossier Médical Personnel
DPO	Délégué à la protection des données à caractère personnel
DSIO	Direction du Système d'Information et de l'Organisation
ES	Etablissement de Santé
GIE	Groupement d'Intérêt Economique
HN	Hôpital Numérique
HOP'EN	Hôpital Numérique ouvert sur son environnement (suite du programme Hôpital Numérique pour la période 2018-2022)
MS Santé	Messagerie Sécurisée de Santé
PAS	Plan d'Actions Sécurité
PCA	Plan de Continuité d'Activité
PGSSI	Politique Générale de Sécurité du Système d'Information : PGSSI-S = PGSSI « de Santé »
PRA	Plan de Reprise d'Activité
PSSI	Politique de Sécurité du Système d'Information
RIL	Référent Informatique et Liberté
RSSI	Responsable de la Sécurité du Système d'Information
SDSI	Schéma Directeur du Système d'Information
SI	Système d'Information
SSI	Sécurité du Système d'Information
SUN-ES	Sécur Numérique Usage en Etablissements de Santé