HÔPITAL NUMÉRIQUE

Programme Hôpital numérique

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ DE LA SANTÉ

Boite à outils pour l'atteinte des pré-requis

Fiches pratiques

Octobre 2012

Direction générale de l'offre de soins

Sommaire

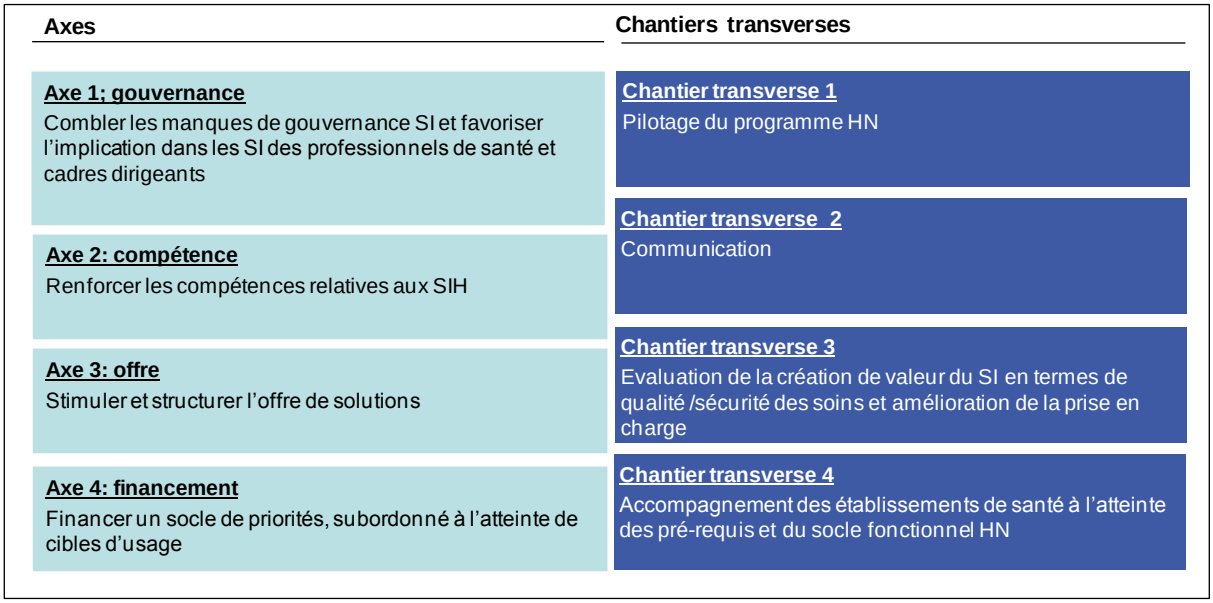
1. LE PROGRAMME HOPITAL NUMERIQUE

Le développement et la modernisation des systèmes d'information hospitaliers (SIH) sont devenus un enjeu majeur pour l'ensemble de la politique d'amélioration de l'organisation des soins. Afin de préparer les prochaines étapes de développement des systèmes d'information hospitaliers au service d'une meilleure prise en charge des patients, la direction générale de l'offre de soins (DGOS) a lancé en novembre 2011 **le programme Hôpital numérique, plan stratégique de développement et de modernisation des SIH pour la période 2012-2016**.

Le programme Hôpital numérique a pour ambition de :

- **Coordonner l'ensemble des acteurs** (établissements de santé, ARS, administration centrale, industriels) autour d'une feuille de route commune pour les SIH ;
- Amener l'ensemble des établissements de santé **à un niveau de maturité de leurs systèmes d'information suffisant pour améliorer significativement la qualité, la sécurité des soins et la performance** dans des domaines fonctionnels prioritaires, sur un socle assurant la sécurité des données ;
- **Soutenir les projets innovants.**

Pour ce faire, le programme Hôpital numérique propose d'agir simultanément sur quatre axes stratégiques et quatre chantiers transverses :



2. LE SOCLE COMMUN DU PROGRAMME

Le programme Hôpital numérique vise à amener, à horizon 2016, l'ensemble des établissements de santé[1] vers un **premier niveau de maturité** de leurs systèmes d'information pour améliorer significativement la qualité, la sécurité des soins et la

[1] *Les établissements de santé concernés par le programme Hôpital Numérique sont les établissements sanitaires quel que soit leur statut (public, privé, ESPIC) et leur champ d'activité (MCO, SSR, PSY, HAD).*

performance dans des domaines fonctionnels prioritaires, sur un socle assurant la sécurité des données.

Ce premier palier de maturité défini par le programme se compose :

- De **3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité :
  - Identité / Mouvement ;
  - Fiabilité / Disponibilité ;
  - Confidentialité.

- De **5 domaines fonctionnels prioritaires**, pour lesquels le programme définit des exigences en matière **d'usage** du système d'information :
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins.
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

L'ensemble des indicateurs associés au socle commun Hôpital numérique est détaillé au sein du « Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun », disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html.

3. LA BOITE A OUTILS POUR L'ATTEINTE DES PRE-REQUIS – LES FICHES PRATIQUES

Afin de les accompagner dans l'atteinte des pré-requis, la DGOS a souhaité les outiller en mettant à leur disposition une boîte à outils composée de :

- **Un outil d'auto diagnostic et plan d'actions associé** permettant aux structures qui le souhaitent de procéder à une auto-évaluation de leur situation au regard des 3 pré-requis du programme et d'identifier sur cette base la démarche et les actions à mettre en œuvre pour atteindre l'ensemble des indicateurs des pré-requis**. Cet outil ainsi que son mode d'emploi sont téléchargeables à l'adresse suivante :** http://www.sante.gouv.fr/programme-hopital-numerique.html;
- **Des fiches pratiques autoporteuses** visant à apporter aux établissements un support méthodologique pour l'atteinte des pré-requis du programme**.**

Les fiches pratiques présentées ci-dessous ont vocation à aider les établissements dans l'atteinte des pré-requis du programme Hôpital numérique en mettant à leur disposition des **documents pratiques et supports méthodologiques**. Ces fiches sont autoporteuses ; elles peuvent être utilisées indépendamment de l'outil d'autodiagnostic et du plan d'actions associé.

Ces fiches pratiques sont les suivantes :

- ***Indicateur P1.2 (Existence d'une cellule d'identitovigilance opérationnelle) : Exemple de méthode de mise en œuvre de l'identitovigilance au sein d'un établissement de santé***

  Cette fiche pratique propose une méthode pour la mise en œuvre d'une démarche d'identito-vigilance au sein d'un établissement de santé. Elle s'appuie en particulier sur les travaux qui ont été menés par le Groupement pour la Modernisation des Systèmes d'Information Hospitaliers (GMSIH) sur l'identification du patient en établissement et la rédaction de la politique d'identification des établissements.

- ***Indicateur P1.4 (Existence d'un référentiel unique de structure piloté et mis à jour régulièrement dans les applicatifs, en temps utile) : Procédure type de mise à jour du référentiel unique de structure***

  Cette fiche pratique propose des modalités de mise à jour du référentiel unique de structure et d'intégration de ces mises à jour dans les applicatifs de l'établissement.

  Cette procédure constitue un document justificatif demandé dans le dossier de candidature de l'établissement au volet « financement » du programme.

- ***Indicateur P2.1 (Existence d'un Plan de reprise d'activité du système d'information formalisé) : Plan type d'un Plan de reprise d'activité du système d'information et bonnes pratiques***

  Ce document propose un plan type d'un Plan de reprise d'activité du système d'information d'un établissement de santé (PRA). Il indique les éléments indispensables qu'il convient d'intégrer dans un PRA du système d'information.

- ***Indicateur P2.2 (Existence d'une définition d'un taux de disponibilité cible des applicatifs et la mise en œuvre d'une évaluation de ce taux) : Exemple de méthode d'évaluation des taux de disponibilité des applications***

  Cette fiche pratique propose une méthode d'évaluation du taux de disponibilité des applications.

- ***Indicateur P2.3 (Existence de procédures assurant d'une part un fonctionnement dégradé du système d'information au cœur du processus de soins en cas de panne et d'autre part un retour à la normale) : Bonnes pratiques d'élaboration des procédures de fonctionnement en mode dégradé et de retour à la normale du système d'information***

  Une proposition de méthode d'élaboration des procédures de fonctionnement en mode dégradé et de retour à la normale du système d'information est présentée dans cette fiche pratique.

- ***Indicateur P3.1 (Existence d'une politique de sécurité formalisée pour les applications au cœur du processus de soins et fondée sur une analyse des risques au sein de l'établissement et l'existence d'une fonction de référent sécurité) : Fiche de poste type d'un Responsable de la sécurité des Systèmes d'information (RSSI) et description des fonctions d'un référent sécurité du système d'information***

  Cette fiche propose une fiche de poste type d'un RSSI détaillant la description des missions et des activités ainsi que le profil et les compétences requis. Elle propose également une description des fonctions d'un référent sécurité d'un établissement de santé.

- ***Indicateur P3.2 (Existence d'une charte ou d'un document formalisant les règles d'accès et d'usage du système d'information, en particulier pour les applications gérant des informations de santé à caractère personnel, diffusé au personnel, aux nouveaux arrivants, prestataires et fournisseurs) : Charte type d'accès et d'usage du système d'information***

  Cette fiche pratique propose une charte type d'accès et d'usage du système d'information, laquelle décrit les règles d'accès et d'utilisation des ressources informatiques et des services Internet d'un établissement et rappelle aux utilisateurs les droits et responsabilités qui leur incombent dans l'utilisation du système d'information.

Les fiches pratiques sont disponibles dans la suite du présent document.

3.1 FICHE PRATIQUE 1 : EXEMPLE DE MÉTHODE DE MISE EN ŒUVRE DE L'IDENTITO-VIGILANCE AU SEIN D'UN ÉTABLISSEMENT DE SANTÉ

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Identités, mouvements » comprend 4 indicateurs, dont l'indicateur P1.2 portant sur **l'existence d'une Cellule d'identito-vigilance opérationnelle**[2]. Cette cellule s'inscrit plus largement dans la mise en œuvre d'une démarche d'identito-vigilance dont cette fiche pratique propose une méthode dans le cadre de l'outillage des établissements de santé par la DGOS.

PRESENTATION DE LA FICHE PRATIQUE

Le présent document propose **une méthode pour la mise en œuvre d'une démarche d'identito-vigilance au sein d'un établissement de santé** ; méthode correspondant à celle du plan d'action proposé aux établissements de santé pour atteindre les pré-requis du programme Hôpital numérique. Il s'appuie en particulier sur les travaux du GMSIH menés sur l'identification du patient en établissement de santé (avril 2002) et sur la rédaction de la politique d'identification des établissements (octobre 2007).

Cette fiche ne constitue pas une recommandation mais vise à présenter aux établissements un cadre méthodologique pour mettre en œuvre une démarche d'identito-vigilance. Elle concerne les aspects techniques de l'identitovigilance et non organisationnels.

[2] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

La méthode qui est proposée dans cette fiche pratique correspond à une démarche globale de mise en œuvre de l'identito-vigilance qui va ainsi au-delà de l'exigence fixée par le programme, laquelle porte sur l'existence d'une cellule d'identito-vigilance opérationnelle[2].

1. REALISATION D'UN ETAT DES LIEUX DE LA GESTION DES IDENTITES AU SEIN DE L'ETABLISSEMENT DE SANTE

La **réalisation d'un état des lieux** constitue un préalable à une meilleure identification du patient au sein de l'établissement. Cet état des lieux s'articule autour de **deux volets**, organisationnel et technique, qui doivent permettre de décrire l'existant et d'envisager les évolutions permettant d'améliorer l'identification du patient au sein de l'établissement.

A. **Le volet organisationnel de l'état des lieux** doit permettre de vérifier l'existence des structures de base au sein de l'établissement pour mettre en place une politique d'identification efficace. Ce premier volet consiste à mener une analyse de l'existant sur les points suivants :
   - Le recensement des lieux où s'effectue l'identification des patients, ainsi que les acteurs impliqués dans l'identification : *Quels sont les services qui identifient les patients ? Qui sont les acteurs responsables de l'identification du Patient ? Existe-t-il une Cellule d'identito-vigilance ? ….*
   - La politique d'identification : A-*t-elle été définie ? Est-elle formalisée ? Est-elle appliquée ? Son application est-elle vérifiée et est-elle mise à jour régulièrement ? …*
   - Les procédures d'identification des patients : *Sont-elles mises en place? Sont-elles diffusées ? Sont-elles appliquées ? Sont-elles mises à jour régulièrement ? Des formations du personnel ont-elles été mises en place ? Des procédures qualité ont-elles été mises en place ? …*
   - Le processus de contrôle de l'identité des patients / de gestion des anomalies des identités et des corrections associées **:** *Ces processus sont-ils définis ? Formalisés ? Appliqués par les acteurs ? …*

B. **Le volet technique de l'état des lieux** vise à vérifier l'état du système d'information participant à l'identification du *patient, afin d'en déduire les évolutions à réaliser. Ce second volet doit pe*rmettre d'aborder les points suivants :
   - La cartographie des systèmes : cartographie des applications, informations relatives aux identités des patients utilisées par ces applications, cartographie des flux mis en œuvre entre ces applications ;
   - Les caractéristiques techniques des outils utilisés et en particulier la définition des interfaces mises en œuvre (mode de communication et contenu des échanges) et des normes et standards supportés par les applications mises en œuvre ;
   - Les éléments de sécurité mis en œuvre ;
   - Les caractéristiques des moyens de communication existants ;
   - Le fonctionnement en mode dégradé des systèmes mis en œuvre ;
   - Les éléments de qualité connus du système comme par exemple le nombre d'identités gérées actives et historiques, le nombre de doublons, ... ;
   - Les éléments de performance connus du système comme par exemple les temps de réponse moyens, le taux de disponibilité du système, ... ;
   - La présence ou non d'un Enterprise Application Integration (EAI) et son périmètre.

L'établissement de santé met en place un **groupe de travail *ad hoc*** pour réaliser cet état des lieux. Ce groupe de travail composé notamment des représentants de la Direction

générale, de la Commission Médicale de l'établissement, de la Direction des systèmes d'information, de la Direction de l'Information Médicale, ainsi que des services de l'établissement utilisateurs du système d'information (service des admissions, service des urgences, laboratoires, …) se réunira régulièrement tout au long de la période de réalisation de l'état des lieux.

2. ELABORATION DE LA POLITIQUE DE GESTION DES IDENTITES DU PATIENT

Sur la base de l'état des lieux de la gestion des identités mené préalablement, l'établissement définit sa politique d'identification et de rapprochement d'identités qu'il formalise respectivement dans une **Charte d'identification** et une **Charte de rapprochement d'identités**.

A. La politique d'identification des patients vise à garantir une identification fiable et de qualité des patients au sein de l'établissement. Cette politique formalisée dans la Charte d'identification de l'établissement définit notamment :

- Le périmètre de la politique : *population de patients concernée, type de prise en charge concerné, périmètre technique, ...* ;
- Les principes et les processus d'identification à respecter : *procédures de création, de contrôle interne et qualité, traçabilité, ...* ;
- Les acteurs concernés et les instances en charge de garantir l'identification du patient ;
- L'organisation mise en œuvre et la répartition des responsabilités ;
- Les outils : *services disponibles, formats utilisés, concepts utilisés, ...*[3].

La politique d'identification de l'établissement de santé devra prendre en compte l'Identifiant National de Santé (INS) mis en place suite aux travaux menés par le GMSIH et dont la gestion et le déploiement sont pilotés par l'ASIP Santé.

Cette Charte doit être cohérente avec les principes énoncés dans la politique de rapprochement lorsque celle-ci existe.

B. La politique de rapprochement d'identités permet d'assurer la cohérence des identités partagées au sein de l'établissement ou d'organisations de santé souhaitant communiquer. Cette politique formalisée dans la Charte de rapprochement d'identités de l'établissement définit notamment :

- Les règles de gestion des rapprochements ;
- Les relations entre domaines et le partage des responsabilités ;
- Le format de l'identifiant et des traits utilisés ;
- Les services disponibles ;
- Les droits d'accès à la structure de rapprochement (habilitations) ;
- Le mode d'authentification des accès (cartes ou autres) ;
- Les normes et standards utilisés ;
- Les principes de sécurisation des données[4].

[3] *GMSIH ; Guide pour l'élaboration des politiques d'identification et de rapprochement ; avril 2002*
[4] *GMSIH ; Guide méthodologique à l'usage des établissements : Réalisation d'un état des lieux de l'identification du patient ; octobre 2007*

Elle doit être cohérente avec la politique d'identification des organisations impliquées. Le cas échéant, elle peut amener à une modification de la politique d'identification.

Ces Chartes sont définies et mises à jour par les **Autorités Gestion de l'Identification / du Rapprochement (AGI / AGR)** mises en place à cet effet. Ces Autorités sont également en charge de l'allocation des moyens nécessaires à la mise en œuvre de ces politiques et l'adaptation de l'organisation permettant d'assurer une identification fiable du patient.
Afin de ne pas multiplier les instances faisant appel à la Direction générale, des établissements ont choisi de confier les missions de ces instances à une structure existante, telle que le Comité de pilotage « Qualité », le Comité « Qualité et gestion des risques », le Collège de l'Information Médicale, le Conseil de la Direction de l'Information Médicale, …[5] .

Dans le cadre de l'élaboration de ces politiques, l'établissement de santé tiendra compte des dispositions du critère 15.a. « Identification du patient à toutes les étapes de sa prise en charge » du manuel de certification v2010 de la Haute Autorité de Santé (HAS)[6]. Il trouvera dans le document décrivant les éléments de vérification des experts-visiteurs, les éléments qu'il veillera à prendre en compte, notamment :

- Elément d'appréciation E1. Une organisation et des moyens permettant de fiabiliser l'identification du patient, à toutes les étapes de sa prise en charge, sont définis ;
- Elément d'appréciation E2. Les professionnels de santé vérifient la concordance entre l'identité du bénéficiaire de l'acte et la prescription avant tout acte diagnostique ou thérapeutique ;
- Elément d'appréciation E3. La fiabilité de l'identification du patient à toutes les étapes de la prise en charge est évaluée à périodicité définie (indicateurs, audits) et les erreurs sont analysées et corrigées.

3. MISE EN PLACE D'UNE CELLULE D'IDENTITO-VIGILANCE

La **Cellule d'identito-vigilance** est l'organe en charge de la surveillance et de la prévention des erreurs et des risques liés à l'identification des patients au sein d'un établissement de santé. Elle est l'instance qui met en œuvre la politique d'identification de l'établissement[7].

Pour mettre en place une Cellule d'identito-vigilance, l'établissement de santé devra dans un premiers temps déterminer et formaliser les éléments suivants :

- Les missions de la Cellule d'identito-vigilance ;
- La composition de la Cellule d'identito-vigilance ;
- Le mode de fonctionnement de la Cellule.

Des recommandations relatives aux missions à confier à la Cellule d'identito-vigilance, à sa composition et son mode de fonctionnement sont proposées ci-après.

---

[5] *Direction Régionale des Affaires Sanitaires et Sociales de Midi-Pyrénées ; Quelques recommandations pour la mise en œuvre de l'identito-vigilance dans les établissements de santé ; juillet 2009*
6 Haute Autorité de Santé (HAS) ; Manuel de certification v2010 – critère 15.a « Identification du patient à toutes les étapes de sa prise en charge » ; Avril 2011

[7] *Cf. fiche pratique « étape 3. Elaboration de la politique de gestion des identités des patients de l'établissement »*

- **Missions de la Cellule d'identito-vigilance**

Les missions de la Cellule d'identito-vigilance sont les suivantes :

- Mettre en œuvre la politique d'identification de l'établissement de santé ;
- Accompagner au quotidien, ou de manière régulière, le bureau des entrées et tous les autres services en charge de l'identification pour le traitement et le suivi des anomalies (doublons, collisions, ...) ;
- Gérer les problèmes liés aux actions d'identification du patient ;
- Transmettre les informations nécessaires aux autres domaines d'identification pour réaliser des rapprochements d'identités ;
- Alerter l'Autorité de gestion de l'identification des éventuels dysfonctionnements dans la mise en œuvre de la politique d'identification;
- Produire, suivre et transmettre à l'Autorité de gestion de l'identification les indicateurs qualités ;
- Elaborer les règles de gestion concernant les services de l'établissement ;
- Conduire des actions de formation, d'assistance et de sensibilisation aux politiques d'identification et de rapprochement auprès de l'ensemble des acteurs de l'établissement ;
- Rédiger des manuels de procédure ;
- Valider ou modifier les actions de rapprochement (mise à jour, fusions, modifications, éclatement) de l'identité, et en informer l'Autorité de gestion des rapprochements qui les répercute dans l'infrastructure centrale et les diffuse à l'ensemble des domaines concernés.

- **Composition de la Cellule d'identito-vigilance**

La Cellule d'identito-vigilance est généralement composée des représentants de l'établissement suivants :

- Le gestionnaire des risques ;
- Le médecin du département de l'information médicale ;
- Un représentant de la direction des systèmes d'information ;
- Un représentant du bureau des entrées ;
- Un représentant de chaque service concerné par l'identification ;
- Les membres du Comité de coordination des vigilances et de gestion des risques ;
- Toute autre personne qualifiée.

- **Fonctionnement de la Cellule d'identito-vigilance**

La Cellule d'identito-vigilance se réunit selon une **périodicité a minima trimestrielle** ou un rythme permettant d'assurer une identification fiable au regard du flux de création. Les échanges tenus au cours de ces réunions sont formalisés dans des comptes-rendus.

Un **système de permanence** peut être assuré par un ou deux membres de la Cellule d'identito-vigilance pour traiter les cas les plus simples. Les cas les plus complexes nécessitant l'intervention du médecin DIM pour consulter les dossiers médicaux sont traités de manière périodique selon les besoins de l'établissement.

La Cellule d'identito-vigilance est **l'administrateur de l'identité** au sein du domaine d'identification. Ses membres disposent donc de l'ensemble des droits sur les services.
Cependant au sein de la Cellule d'identito-vigilance, seul un professionnel de santé tenu au secret médical et ayant les compétences médicales adéquates dispose de l'**habilitation nécessaire pour consulter les informations complémentaires du patient de nature médicale**.

Enfin, la Cellule d'identito-vigilance élabore **un rapport d'activité** recensant notamment les actions menées pour la mise en œuvre de la politique de gestion des identités (élaboration de procédures, actions de communication, formation, ...) et les indicateurs d'évaluation de la qualité de l'identification des patients par les acteurs de l'établissement.

4. MISE EN ŒUVRE DE LA POLITIQUE DE GESTION DES IDENTITES PAR LA CELLULE D'IDENTITO-VIGILANCE

La Cellule d'identito-vigilance une fois mise en place met en œuvre la politique d'identification et de rapprochement d'identités de l'établissement.

Pour mener à bien son activité, la Cellule d'identito-vigilance est notamment accompagnée du gestionnaire des risques et du Comité de coordination des vigilances et de gestion des risques de l'établissement.

Les activités de la Cellule sont les suivantes :

- **Elaboration des procédures d'identification et de rapprochement d'identités**

  La Cellule d'identito-vigilance rédige et établit des procédures ayant pour objectif d'appliquer la politique d'identification et de rapprochement d'identités de l'établissement. Ces procédures décrivent notamment les processus d'identification du patient tels que la création, la validation ou la recherche d'une identité.

- **Mise en place de plans de communication et de formation au sujet de l'identification auprès du personnel de l'établissement de santé**

  Afin de sensibiliser le personnel de l'établissement de santé aux enjeux de l'identification du patient et porter à sa connaissance la politique d'identification de la structure, la Cellule d'identito-vigilance met en œuvre des actions de communication et de formation.

  Deux actions de sensibilisation et de formation doivent être envisagées :

  - **Une action d'information et de communication générale** afin que l'ensemble des acteurs soit sensibilisé aux enjeux de l'identification (sessions d'information, affiches de communication).
  - **Une action de formation spécifique à l'utilisation des outils au quotidien** à destination du personnel concerné (sessions de formation, assistance téléphonique, aide en ligne, ...).

- **Mise en place d'un système d'évaluation et d'un suivi qualité**

  La Cellule d'identito-vigilance produit et analyse périodiquement un tableau de bord recensant des indicateurs de qualité. Parmi ceux-ci pourront être suivis :

- **Les indicateurs portant sur la qualité des données** (taux de doublons, taux de collisions, taux de modifications de l'identité, taux d'identités créées à l'état provisoire, ...) ;
- **Les indicateurs portant sur l'utilisation des services** (taux de fusions, classement des informations le plus fréquemment accédées, ...) ;
- **Les indicateurs portant sur l'organisation de l'identification** (taux de fusions par service, classement des informations le plus fréquemment accédées par service, ...).

Ces indicateurs permettent d'évaluer le niveau de qualité de l'identification des patients au sein de l'établissement et la bonne application de la politique d'identification par les acteurs.

En complément de ces activités, la Cellule d'identito-vigilance peut également être amenée à réaliser en collaboration avec d'autres acteurs la définition d'une architecture technique cible du système d'identification du patient, ainsi que l'adaptation des applications « métier » existantes.

L'établissement veillera à mettre en place une gestion structurée de la documentation relative à la politique d'identification des patients au sein de la structure (charte d'identification, charte de rapprochement, procédures associées, etc.).

5. POUR ALLER PLUS LOIN

Dans le cadre de la mise en place de sa démarche d'identito-vigilance, l'établissement de santé pourra notamment s'appuyer sur les documents suivants :

- HAS ; Guide pour préparer et conduire votre démarche de certification V2010 : Elément de vérification des critères PEP ; juin 2011
- GMSIH ; Accompagnement à la rédaction de la politique d'identification des établissements de santé ; Octobre 2007
- GMSIH ; Evaluer l'existant organisationnel et technique mis en place par mon établissement (identification du patient ; Octobre 2007 ;
- GMSIH ; Travaux relatifs à l'identification du patient ; Avril 2002 ;
- Groupe de travail de la CCREVI de Midi-Pyrénées ; Quelques recommandations pour la mise en œuvre de l'identito-vigilance dans les établissements de santé ; Juillet 2009 ;
- Collège National de Biochimie des Hôpitaux ; Guide pratique de l'identitovigilance ; Septembre 2012

3.2 FICHE PRATIQUE 2 : PROCÉDURE TYPE DE MISE À JOUR DU RÉFÉRENTIEL UNIQUE DE STRUCTURE

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Identités, mouvements » comprend 4 indicateurs, dont l'indicateur P1.4 portant sur **l'existence d'un référentiel unique de structure de l'établissement piloté et mis à jour régulièrement dans les applicatifs, en temps utile**[8].

Dans le cadre de l'outillage des établissements de santé pour l'atteinte des pré-requis du programme Hôpital numérique, la DGOS met à la disposition des établissements une fiche pratique relative à la procédure de mise à jour du référentiel unique de structure.

PRESENTATION DE LA FICHE PRATIQUE

La procédure de mise à jour du référentiel unique de structure de l'établissement vise à décrire les modalités d'actualisation du référentiel susvisé d'une part, et le mode d'intégration de ces mises à jour dans les applicatifs d'autre part.

Le présent document constitue une procédure type élaborée sur la base de documents transmis par des établissements de santé. Cette fiche concerne le découpage interne de l'établissement uniquement, mais n'exclut pas la cohérence avec d'autres sources de données.

Pour accompagner les établissements dans **l'élaboration et la formalisation d'une procédure de mise à jour du référentiel unique de structure** (à partir de la présente fiche pratique) adaptée à leur organisation, sont distingués ci-après dans le document par un code couleur :

[8] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

- En violet encadré, des explications sur l'objet et le contenu d'un paragraphe, ainsi que des informations ayant vocation à accompagner l'établissement dans l'élaboration de sa propre procédure. Ces indications doivent être supprimées du document avant sa diffusion ;
- En bordeaux, des informations propres à chaque établissement. Ces informations doivent donc être renseignées et contextualisées par la structure lors de l'élaboration de sa propre procédure ;
- **En noir, des éléments d'ordre générique qui peuvent constituer la base de la procédure de mise à jour du référentiel de structure de l'établissement de santé.**

Pour aller plus loin, l'établissement de santé pourra se référer aux documents suivants :

- Direction Générale de l'Offre de Soins (DGOS) ; Guide méthodologique de comptabilité analytique hospitalière ;
- Agence Technique de l'Information Hospitalière (ATIH) ; Guides méthodologiques de production du PMSI ;
- GMSIH ; Référentiels SID des ES – Synthèse globale - Bien gérer ses référentiels de données : Un enjeu pour mieux piloter la performance de son établissement ; pages 23-30 ; octobre 2008 ;
- Agence Régionale de l'Hospitalisation (ARH) Aquitaine ; Formation Fichier structure ; 22 février 2008 ;

Intitulé de la procédure	PROCEDURE DE MISE A JOUR DU REFERENTIEL UNIQUE DE STRUCTURE

1. OBJET DE LA PROCEDURE

La présente procédure a pour objectif de décrire le **processus de mise à jour du référentiel unique de structure du** *[nom de l'établissement de santé]*. Elle précise d'une part, les modalités de mise à jour du référentiel susvisé et d'autre part, le mode d'intégration de ces mises à jour dans les applicatifs.

2. PERIMETRE DE LA PROCEDURE

Cette section décrit les types de structure et les acteurs concernés par la présente procédure. Elle sera adaptée par l'établissement en fonction de l'organisation interne qu'il aura choisi de mettre en place pour maintenir à jour le référentiel unique de structure et les données associées contenues dans les applicatifs présentée au point 3. « Organisation interne et responsabilités » ci-dessous.

Cette procédure s'adresse au **Référent et à la Cellule en charge de piloter le référentiel unique de structure de l'établissement de santé** (*cf. point 3. « Organisation interne et responsabilités » du document – présentation du Référent et de la Cellule*).

Elle concerne l'ensemble des **structures juridiques, géographiques et fonctionnelles de l'établissement**, lesquelles sont recensées dans le fichier unique de structure.

3. ORGANISATION INTERNE ET RESPONSABILITES

La présente section décrit l'organisation interne retenue par l'établissement pour maintenir à jour le référentiel unique de structure et les données associées dans les applicatifs. La proposition d'organisation ci-dessous sera donc adaptée par l'établissement en fonction de celle qu'il aura choisi de retenir.

Il pourra par ailleurs ajouter ici toute autre information portant sur les responsabilités confiées aux acteurs qui sera jugée pertinente.

Le **Directeur de l'établissement de santé** est le garant de l'application de la présente procédure.

Un Référent est désigné, parmi les professionnels de l'établissement exerçant au sein de la Direction des affaires financières ou de la Direction des systèmes d'information, **afin d'assurer le pilotage du référentiel unique de structure**. Ce Référent a notamment pour missions de :

- Réaliser un état des lieux des structures juridiques, géographiques et fonctionnelles de l'établissement de santé ;
- Réaliser un état des lieux des différents fichiers qui contiennent les structures ainsi que des procédures de mise à jour de ces fichiers ;
- Choisir un fichier de structure comme référentiel unique et préciser le modèle retenu pour décrire les structures ;
- Définir et mettre en œuvre la procédure de mise à jour du référentiel unique de structure ;
- Définir et mettre en œuvre les procédures de mises à jour dans les autres fichiers de structure qu'ils soient ou non dans des applicatifs ;
- Veiller à la cohérence entre le référentiel unique de structure et les fichiers de structure utilisées par les applicatifs de l'établissement de santé ; mettre en place et conduire des vérifications périodiques de la cohérence ;
- Alerter les acteurs de l'établissement en cas d'absence de cohérence entre les données d'un applicatif et celles du référentiel unique de structure.

Ce Référent participe à **une Cellule mise en place pour proposer les décisions à prendre concernant les évolutions relatives à l'organisation de l'établissement et au fichier unique de structure associé** *(ex : création d'une Unité Fonctionnelle (UF), validation des mises à jour du fichier unique de structure, …)*. Les décisions relatives à l'organisation de l'établissement, telles que la création d'une UF, relevant en dernière instance de la Direction des affaires financières et de la commission médicale de l'établissement réunies en instance ou *[indiquer toute autre instance mise en place à cet effet au sein de l'établissement]*.

Cette Cellule est transverse à l'établissement, sa composition est adaptée et dimensionnée à la mission qu'elle porte de proposition d'arbitrage des évolutions sur l'organisation de l'établissement. Elle est composée de représentants :

- De la Direction des affaires financières ;
- De la Direction des systèmes d'information ;
- Du Département de l'Information Médicale ;
- De la Direction des Soins ;
- De la Direction de la Qualité ;
- Des services de soins et administratifs de l'établissement ;
- Du service informatique ;
- *[L'établissement ajoutera ici tout autre acteur qu'il souhaite intégrer dans la Cellule]*.

La Cellule se réunit *a minima* à un rythme semestriel ou un rythme permettant de maintenir à jour le référentiel, ainsi que les données associées dans les applicatifs.

4. MODE OPERATOIRE

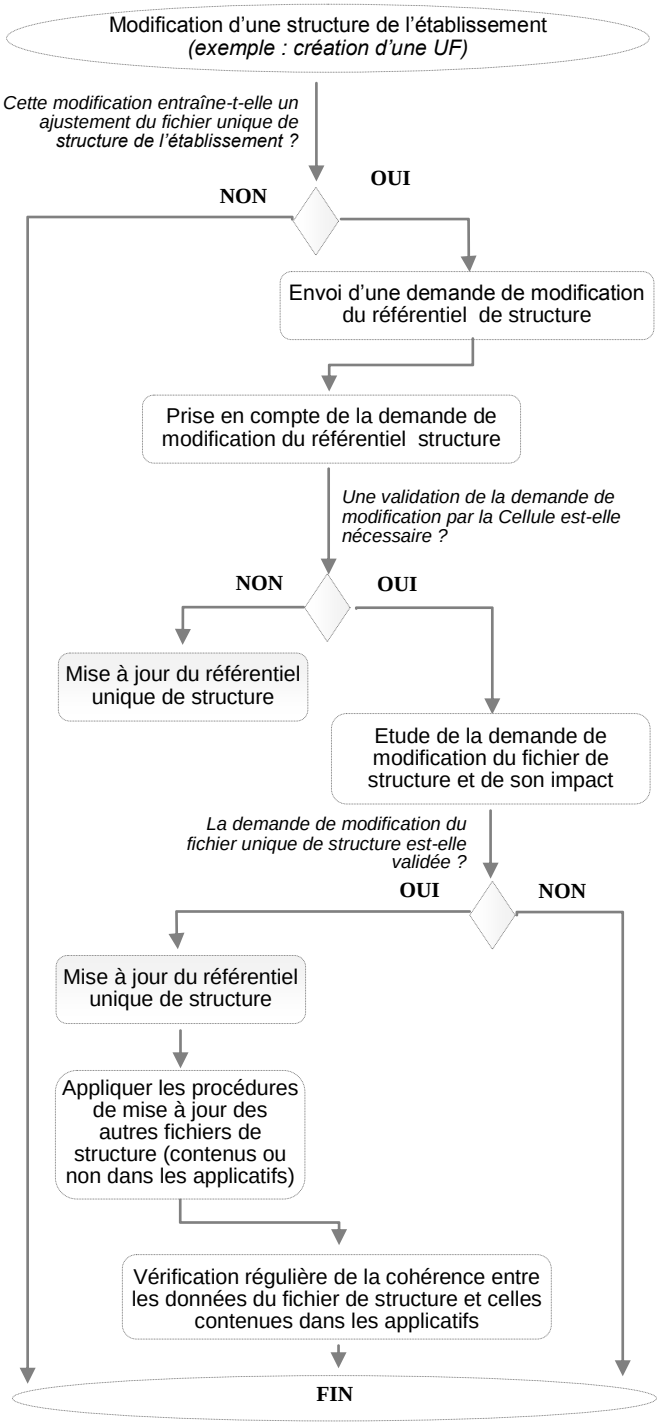
Cette section présente le mode opératoire de mise à jour du référentiel unique de structure et des données associées contenues dans les applicatifs tel que définis par l'établissement.

Une proposition de mode opératoire est présentée ci-dessous ; celle-ci sera adaptée par l'établissement en fonction du processus qu'il souhaite mettre en place pour maintenir à jour le référentiel unique de structure et les données associées dans les applicatifs.

Enfin, il pourra être ajouté dans la présente section toute information jugée pertinente par l'établissement.

Le processus de mise à jour du référentiel unique de structure de l'établissement de santé et des autres fichiers de structure (contenus ou non dans les applicatifs) est présenté en page suivante.

QUI ?	QUOI ?	COMMENT ?
DAF / DSI	Envoi d'une demande de modification du référentiel de structure	Formulaire de demande de modification du fichier unique de structure de l'établissement
Référent du référentiel unique de structure	Prise en compte de la demande de modification du référentiel structure	
Cellule *ad hoc* de gestion des structures de l'établissement	Mise à jour du référentiel unique de structure	Mise à jour du référentiel de structure
	Etude de la demande de modification du fichier de structure et de son impact	Tenue d'une réunion de la Cellule *ad hoc*
Référent du référentiel unique de structure	Mise à jour du référentiel unique de structure	
	Appliquer les procédures de mise à jour des autres fichiers de structure (contenus ou non dans les applicatifs)	Appliquer la procédure de mise à jour technique du fichier référentiel des structures
	Vérification régulière de la cohérence entre les données du fichier de structure et celles contenues dans les applicatifs	



Toute modification effectuée dans le référentiel unique de structure sera systématiquement communiquée par voie de note interne ou électronique aux acteurs de l'établissement de santé ayant recours à ces informations dans le cadre de leur activité professionnelle :

- Les agents de la Direction des affaires financières de l'établissement ;
- Les agents de la Direction du système d'information ;
- Les agents du Département de l'Information Médicale ;
- Les agents concernés par les modifications apportées au référentiel unique de structure ;
- *[L'établissement ajoutera ici tout autre acteur auquel les informations de modification du fichier unique de structure et des données associées dans les applicatifs doivent être communiquées]*.

Par ailleurs, les modifications ayant un impact sur la structure de l'établissement seront également communiquées aux acteurs externes concernés (ex : tutelles, autres intervenants extérieurs si nécessaire).

L'établissement précisera également ici la fréquence à laquelle il souhaite procéder à la mise à jour des données contenues dans le référentiel unique de structure et dans les applicatifs. En fonction des besoins de l'établissement, cette mise à jour pourra se faire soit au fil de l'eau, soit à des périodes régulières prédéfinies *(chaque trimestre par exemple)*.

De plus, en fonction du volume de mises à jour à effectuer, l'établissement pourra choisir d'effectuer une mise à jour manuelle ou automatique des données présentes dans les applicatifs.

5. PROPAGATION DES MISES A JOUR AU SEIN DU SYSTEME D'INFORMATION

Cette section décrit le mode de propagation des modifications effectuées dans le référentiel unique de structure au sein du système d'information retenu par l'établissement de santé.

Plusieurs modes de propagation peuvent coexister, selon les applications et selon le type de modifications à apporter (évolutions mineures des structures existantes, ou refonte majeure). Il s'agit de décrire chaque mode de propagation possible, les applications concernées, ainsi que les règles d'application de chacun.

La propagation des modifications peut se faire par exemple :

- Au fil de l'eau dans le cas de modifications mineures :

> Manuellement : dans ce cas, les évolutions sont reportées manuellement dans chaque application en utilisant l'interface utilisateur propre à chacune ;

> De façon automatique pour les applications qui le permettent (par exemple, par une interface entre l'application qui gère le référentiel de structure et les applications connectées).

- Ponctuellement, pour des modifications importantes :

> Il peut d'agir alors d'importer tout ou partie de la structure, en remplacement de la structure existante ;

> Ou par l'interface si une telle interface est disponible entre le référentiel et les applications connectées.

Les modalités de gestion des historiques seront également à définir. Il est nécessaire de conserver dans le référentiel de structure, les structures actives « en cours », mais également les structures qui ont été fermées, et de tracer l'historique des modifications (création, fermeture, modification des attributs de la structure).

La cible à rechercher par l'établissement de santé est la mise en place d'un référentiel unique de structure alimentant les différentes applications du SIH afin d'éviter les contrôles manuels et les mises en cohérence manuelles entre les différents fichiers.

6. SUIVI DE LA MISE EN ŒUVRE DE LA PROCEDURE

Cette section présente les modalités de suivi de la mise en œuvre de la procédure. Elle sera donc adaptée aux modalités de suivi que souhaite mettre en œuvre l'établissement de santé.

Toute autre information jugée pertinente pourra être ajoutée par l'établissement de santé.

Une **vérification de la bonne application de la présente procédure** par les acteurs concernés est effectuée à un rythme semestriel ou permettant de garantir la cohérence des données des différents fichiers de structure (contenus ou non dans des applications) avec celles du référentiel unique de structure de l'établissement.

Cette vérification est menée par le **Référent en charge du pilotage du référentiel unique de structure**. Elle consiste en la réalisation d'un audit sur un échantillon d'applications.

A l'issue de l'audit, un **rapport** est élaboré par le Référent. Celui-ci contient les informations suivantes :

- Le périmètre de l'audit *(structures et applications auditées, …)* ;
- La présentation des mises à jour réalisées sur la période *(ajouts, corrections de données existantes, …)*;
- Le rappel des décisions prises par la Cellule concernant la structure de l'établissement et le fichier unique associé *(adaptation du modèle, revue de la procédure de mise à jour, …)* ;
- La description des éventuelles incohérences identifiées ;
- Les indicateurs de suivi de la mise en œuvre de la Procédure *(cf. liste des indicateurs de suivi ci-dessous)*.

Parmi ces indicateurs sont notamment suivis :

- Le nombre de décisions de mise à jour prises par la Cellule et la description de ces décisions ;
- Le nombre de mises à jour effectuées sur la période *(ajout de structure, correction de données, …)* ;
- Le nombre d'incohérences identifiées entre les données issues du fichier unique de structure et celles contenues dans les applicatifs ;
- *[L'établissement ajoutera tout autre indicateur qu'il juge pertinent de suivre pour évaluer l'application de la procédure]*.

3.3 FICHE PRATIQUE 3 : PLAN TYPE D'UN PLAN DE REPRISE D'ACTIVITÉ DU SI ET BONNES PRATIQUES

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Fiabilité, disponibilité » comprend 3 indicateurs, dont l'indicateur P2.1 portant sur **l'existence d'un Plan de Reprise d'Activité (PRA) du système d'information formalisé**[9].

Dans le cadre de l'outillage des établissements de santé pour l'atteinte des pré-requis du programme Hôpital numérique, la DGOS met à la disposition des établissements une fiche pratique détaillant le plan d'un PRA du système d'information.

PRESENTATION DE LA FICHE PRATIQUE

La présente fiche pratique propose un plan type d'un PRA du système d'information d'un établissement de santé. Le PRA du système d'information a pour objectif de décrire les dispositions prévues par un établissement pour assurer la reprise de l'activité de son système d'information en cas de crise majeure ou importante du centre informatique.

Pour accompagner les établissements de santé dans **l'élaboration et la formalisation d'un PRA** (à partir du présent Outil pratique) sont distingués ci-après dans le document par un code couleur :

- En violet encadré, des explications sur l'objet et le contenu d'un paragraphe, ainsi que des informations ayant vocation à accompagner l'établissement de santé dans l'élaboration d'un PRA adaptée à ses spécificités. Ces indications doivent être supprimées du PRA avant sa publication.

[9] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

- En bordeaux, des informations propres à chaque établissement. Ces informations doivent donc être renseignées et contextualisées par la structure lors de l'élaboration de son propre PRA.

- **En noir, des éléments d'ordre générique qui peuvent constituer la base du PRA de l'établissement de santé. Ces éléments peuvent être modifiés / complétés selon le contexte et les spécificités du système d'information de l'établissement.**

- En vert, des exemples permettant d'aider les établissements de santé à renseigner le contenu du PRA. Ces exemples doivent être supprimés du document avant sa publication.

1. OBJET DU DOCUMENT

Le présent document a pour objectif de décrire le sommaire du Plan de Reprise d'Activité (PRA) du système d'information. Le document liste le minimum de dispositions que doit prévoir l'établissement pour assurer la reprise de l'activité de son système d'information en cas de crise majeure ou importante du centre informatique.

Ce document présente les questions à se poser relatives aux points suivants :

- **Les applications « métier » exploitées par l'établissement de santé**;
- **Le plan de sauvegarde des données contenues dans le système d'information de l'établissement ;**
- **Les procédures de fonctionnement des applications en mode dégradé (en cas de dysfonctionnements) et les procédures de retour à la normale ;**
- **Les modalités de redémarrage du système d'information en cas de panne** ;
- **L'information des utilisateurs**

2. INFRASTRUCTURE FONCTIONNELLE

2.1 PRESENTATION DE L'ARCHITECTURE APPLICATIVE

Cette section vise à décrire le patrimoine applicatif de l'établissement de santé. La cartographie applicative du système d'information pourra ainsi être intégrée ici.

Par ailleurs, l'établissement pourra s'appuyer sur les travaux qui auront été menés dans le cadre du programme Hôpital numérique sur la cartographie applicative pour compléter ce paragraphe *(i.e. indicateur P1.1. Taux d'application au cœur du processus de soins, de la gestion administrative du patient et du PMSI connectées à un référentiel unique d'identités des patients)*.

2.2 CLASSIFICATION DES APPLICATIONS EXPLOITEES

Cette section indique pour chaque application exploitée par l'établissement de santé son niveau de disponibilité et si celle-ci est externalisée ou non. Les applications sont organisées dans le tableau ci-dessous par domaine fonctionnel. Les informations suivantes seront notamment renseignées dans le tableau ci-dessous :

- Domaine : nom du domaine fonctionnel auquel appartient l'application décrite;
- Fonctionnalité : nom de la fonctionnalité à laquelle appartient l'application décrite ;
- Application : nom de l'application décrite ;
- Editeur : nom de l'éditeur de l'application décrite ;
- Besoin en disponibilité : besoin en disponibilité de l'application décrite sur une échelle de 1 à 4 (cf. fiche pratique 4 du présent document) ;
- Externalisation : indiquer si l'application décrite est externalisée ou non (Oui/Non)

Une illustration est proposée ci-dessous afin d'aider l'établissement à renseigner le tableau.

L'établissement de santé pourra par ailleurs s'appuyer sur les travaux qui auront été menés dans le cadre du programme Hôpital numérique sur la mesure du taux de disponibilité des applications pour compléter ce tableau *(i.e. indicateur P2.2. Définition d'un taux de disponibilité cible des applicatifs et mise en œuvre d'une évaluation de ce taux)*.

Enfin, il pourra être ajouté dans la présente section toute information relative aux applications exploitées qui sera jugée pertinente par l'établissement de santé.

[Indiquer le nom de l'établissement de santé] exploite les applications listées dans le tableau ci-dessous. Pour chacune de ces applications, classées par domaine fonctionnel, sont précisés le besoin de disponibilité et l'éventuelle externalisation de celle-ci.

Les domaines fonctionnels indiqués dans le tableau ci-dessous sont ceux utilisés dans l'observatoire des Systèmes d'Information Hospitaliers oSIS.

DOMAINE	FONCTIONNALITÉ	APPLICATION	EDITEUR	BESOIN EN DISPONIBILITÉ	EXTERNALISATION
Gestion administrative du patient		Application A	Editeur A	Sur une échelle de 1 à 4	Oui
		Application B	Editeur B	Sur une échelle de 1 à 4	Non
Gestion du dossier patient (médical et paramédical)					
Gestion des resources					
Gestion des					

prescriptions et demandes d'examens					
Gestion des activités médico-techniques					
Urgences					
Recueil d'activités, production des données T2A					
Système d'information économique et financier					
Système d'information logistique et technique					
Gestion des identités					
Gestion des Ressources Humaines					
Système d'information Qualité et Gestion des risques					
Système d'information de pilotage					
Système d'information de Réseau Ville – Hôpital / Hôpital – Hôpital					
[Nom du domaine fonctionnel]					

Cette liste permet avant tout, sur la base des besoins en disponibilité, de définir un ordre de priorité dans le redémarrage des applications. Ensuite, pour affiner l'ordre de redémarrage, il faut prendre en compte les interactions et dépendances entre applications.

3. DISPOSITIONS PREVUES POUR LA RECUPERATION DES DONNEES

Cette section décrit les mécanismes prévus par l'établissement de santé – et le cas échéant, les sociétés en charge de la maintenance du système d'information de la structure – pour permettre la récupération des données du système d'information perdues.

3.1 PLAN DE SAUVEGARDE DES DONNEES

L'établissement définit tout d'abord le plan de sauvegarde des données contenues dans le système d'information. Pour ce faire, il pourra s'appuyer sur le tableau ci-dessous qui recense les informations suivantes :

- Plateforme : nom de la plateforme de sauvegarde des données ;
- Type de plateforme : type de plateforme de sauvegarde des données ;
- Type de sauvegarde (incrémentale / totale) : sauvegarde des données distinctes par rapport à la précédente sauvegarde uniquement / sauvegarde de l'ensemble des données ;
- Planification (incrémentale / totale) : périodicité, jour et heure de la sauvegarde des données.

Afin de renseigner ce tableau, l'établissement de santé pourra se référer aux Contrats conclus avec les sociétés en charge de la maintenance du système d'information pour recueillir ces informations.

La sauvegarde des données contenues dans le système d'information de l'établissement est placée sous la responsabilité de *[nom de l'établissement / nom des sociétés en charge de la maintenance du système d'information ou nom de la personne de l'établissement].*

Les dispositifs de sauvegarde des données détenus par l'établissement sont ici décrits :

– *[Présenter ici les dispositifs de sauvegarde dont dispose l'établissement de santé (exemples : boitier de sauvegarde, robot, …)] ;*

Le tableau ci-dessous présente le plan de sauvegarde des données de l'établissement:

PLATEFORME	TYPE DE PLATEFORME	TYPE DE SAUVEGARDE		PLANIFICATION DE LA SAUVEGARDE DES DONNEES		PLANIFICATION DES TESTS DE RECUPERATION DES DONNEES	
		Incrémentale	*Totale*	*Incrémentale*	*Totale*	*Incrémentale*	*Totale*
ANAPATH2	Windows serveur 2003	Totales_VLS2	Incrémentales_VLS	3 fois par jour 8h – 12h – 20h	Tous les vendredis 20h30	Tous les mois	Tous les mois

3.2 PROCEDURES DE RECUPERATION DES DONNEES

Une fois le plan de sauvegarde des données élaboré, l'établissement élabore les procédures de récupération des données en fonction des types de sauvegarde qui auront été définis préalablement dans le plan de sauvegarde (i.e. sauvegarde incrémentale ou sauvegarde totale).

Ces procédures précisent notamment les points suivants :

- Diagnostic de la perte de données : nature et volume des données perdues, ampleur et gravité de la perte, … ;
- Détermination des données à récupérer en fonction des données perdues et des sauvegardes disponibles : définir parmi les sauvegardes existantes celles à restaurer (par exemple la dernière sauvegarde incrémentale, ou restauration complète en reprenant la dernière sauvegarde totale suivie des sauvegardes incrémentales)
- Mode de mise en œuvre de la récupération des données : actions à mener, délai de réalisation, tests de vérification de la bonne récupération des données prévus, … ;
- Modalités d'information des utilisateurs : nature de l'information communiquée (données perdues / sauvegardées / récupérées), support de communication utilisé, durée estimée de la perte de données, …

Les procédures de récupération des données devront être élaborées en tenant compte des dispositions du plan de sauvegarde des données qui aura été définit au préalable par l'établissement de santé.

Les procédures de récupération et de sauvegarde doivent être testées périodiquement.

4. DISPOSITIONS PREVUES POUR LE FONCTIONNEMENT DES APPLICATIONS EN MODE DEGRADE ET LE RETOUR A LA NORMALE

Voir la fiche pratique n°5 de la boite à outils pour l'atteinte des pré-requis (bonnes pratiques d'élaboration des procédures de fonctionnement en mode dégradé / de retour à la normale du système d'information).

5. DISPOSITIONS PREVUES POUR LE REDEMARRAGE DES APPLICATIONS

Cette section présente la procédure retenue par l'établissement de santé pour permettre le redémarrage en cas de panne des applications qu'il exploite.

L'établissement de santé contiendra notamment dans cette procédure les points suivants :

- Le diagnostic du (des) dysfonctionnement(s) ayant entraîné une panne des applications ;
- Les modalités de redémarrage : restauration des données puis redémarrage des applications, dans un ordre défini, en fonction des priorités (selon les besoins en

disponibilité) et des indications données par les éditeurs des solutions exploitées. Empêcher par exemple toute connexion au système par les utilisateurs durant la durée de l'intervention

- La vérification du bon fonctionnement des applications : procédure de vérification à prévoir dans l'environnement de production avant d'informer les utilisateurs que les applications sont de nouveau disponibles (ce n'est pas une procédure de tests qui elle se fait dans un environnement de test, mais une procédure de vérification qui garantisse que toutes les fonctions sont rétablies en production)

6. INFORMATION DES UTILISATEURS EN CAS DE PANNE

Cette section définit la procédure d'information des utilisateurs en cas de panne du système d'information qui auront été définies par l'établissement de santé

Cette procédure s'articule notamment autour des points suivants :

1. Information des utilisateurs de l'indisponibilité du système d'information

Ce point précise les informations qui seront communiquées aux utilisateurs en cas d'indisponibilité du système d'information de l'établissement : la nature du dysfonctionnement rencontré, les ressources informatiques indisponibles, la durée de leur indisponibilité, la date prévisible de la résolution du dysfonctionnement, …

Il précise également le support de communication de cette information aux utilisateurs (exemples : messagerie électronique, téléphone, note de service,…

2. Information des utilisateurs de la reprise d'activité du système d'information

Ce point de la procédure a pour objectif de préciser l'information communiquée aux utilisateurs lors de la reprise d'activité du système d'information : les modalités de résolution du dysfonctionnement, la date et l'heure de reprise d'activité du système, les données qui ont été récupérées / perdues, …

Il précisera également la démarche que devront suivre les utilisateurs en cas de difficultés dans le fonctionnement des applicatifs redémarrés : précautions de redémarrage, personnes à contacter, …

7. POUR ALLER PLUS LOIN

Pour compléter le PRA du système d'information, l'établissement de santé pourra notamment intégrer des informations relatives :

- A l'infrastructure technique de l'établissement de santé : cartographie de l'infrastructure technique, lieu géographique de l'infrastructure, description de la salle informatique, du centre d'hébergement, … ;

- Aux principes de sécurité qu'il aura définis pour garantir la continuité d'activité et le retour à la normale du système d'information en cas de panne : sécurité des serveurs, supervision et contrôle, protection logicielle, stockage, …

7.1 INFRASTRUCTURE TECHNIQUE

7.1.1 Présentation de l'architecture technique

Cette section décrit les ressources techniques de l'établissement de santé. La cartographie technique du système d'information pourra ainsi être ici intégrée.

Pourront également être précisées des informations relatives à la liste des serveurs exploités : serveur de données, d'application, serveurs disponibles par environnement, …

7.1.2 Lieu géographique

Cette section présente la localisation géographique de l'infrastructure technique de l'établissement de santé, selon que celle-ci soit hébergée sur un site unique, ou réparti sur des lieux géographiques distincts.

Il convient donc de ne conserver ici que le paragraphe correspondant à la situation de l'établissement de santé, puis de le renseigner des informations indiquées.

- Votre établissement a confié l'hébergement de son système d'information à un tiers :

L'infrastructure technique du ***[nom de l'établissement de santé]*** est hébergée par ***[nom de la société en charge de l'hébergement de l'infrastructure technique de l'établissement]*.**

Elle est ***[localisée sur un seul site géographique / réparti(e) sur plusieurs sites comme suit :***

- ***Localisation géographie de la salle informatique ;***
- ***Localisation géographique du centre d'hébergement (le site de production et le site de secours).***

- Votre établissement héberge le système d'information :

L'établissement de santé héberge lui-même l'infrastructure technique. Celle-ci est ***[localisée sur un seul site géographique / réparti(e) sur plusieurs sites géographiques comme suit :***

- ***Localisation géographique de la salle ou des salles informatique ;***

7.1.3 Description des locaux

Cette section présente les caractéristiques de sécurisation des locaux qui hébergent l'infrastructure technique de l'établissement de santé. Pour chaque local identifié, les informations suivantes sont notamment précisées :

- La sécurisation de l'accès aux locaux ;
- L'alimentation électrique ;

- La climatisation ;
- La sécurité en cas de dégâts des eaux ;
- La détection d'incendie.

L'établissement de santé ajoutera ici toute information sur les caractéristiques de sécurisation des locaux hébergeant l'infrastructure technique qu'il juge pertinent d'intégrer au présent PRA.

De plus, il ajoutera en tant que de besoin les autres locaux qui n'hébergent pas l'infrastructure technique de l'établissement mais qui pourraient avoir un impact sur le fonctionnement des équipements de l'infrastructure technique (ex : salle de l'auto commutateur).

Les caractéristiques générales de sécurisation de la salle informatique sont présentées ci-après.

- ***La sécurisation de l'accès à la salle informatique***

Les informations suivantes sur la sécurisation de l'accès à la salle informatique seront notamment indiquées :

- La localisation de la salle informatique (site géographique, emplacement au sein de l'établissement, …) ;
- Le mode de sécurisation de l'accès à la salle informatique (porte blindée, digicode, alarme, caméra de surveillance, contrôle des mouvements, …)

- ***L'alimentation électrique***

Les informations suivantes sur le système d'alimentation électrique seront notamment indiquées :

- La présence d'onduleurs permettant d'assurer le fonctionnement du système en cas de coupures ;
- La présence de groupes électrogènes de secours en cas de coupures d'électricité ;
- Les modalités de remontée d'alertes en cas de coupures d'électricité ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

Le bureau (la personne) responsable de la maintenance du système d'alimentation électrique

- Les dispositions du contrat de maintenance du système.

- ***La climatisation***

Les informations suivantes sur le système de climatisation seront notamment indiquées :

- La puissance du système de climatisation ;
- La température à laquelle est gardée la salle informatique ;
- Les modalités de remontée d'alertes en cas d'arrêt du système de climatisation ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

Le bureau (la personne) responsable de la maintenance du système de climatisation ;

- Les dispositions du contrat de maintenance du système de climatisation.

- ***La sécurité en cas de dégâts des eaux***

Les informations suivantes sur la sécurité mise en place en cas de dégâts des eaux seront notamment indiquées :

- Les modalités d'alerte en cas de présence d'eau (ex : système de détection, vase de rétention d'eau, …) ;
- L'équipement installé pour évacuer l'eau (ex : pompes de refoulement, …) ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système d'alertes et de l'équipement.

- ***La détection d'incendie***

Les informations suivantes sur le système de détection d'incendie seront notamment indiquées :

- L'équipement mis en place pour détecter / éteindre un incendie ;
- Les procédures de tests mises en œuvre pour vérifier le bon fonctionnement du système ;

Le bureau (la personne) responsable de la maintenance du système de détection d'incendie ;

- Les dispositions du contrat de maintenance du système de détection et d'extinction d'incendie.

7.1.4 Réseau et transport de données

Les informations suivantes sur le réseau de l'établissement de santé et les modalités de transport des données pourront notamment décrites :

- L'architecture du réseau (topologie du réseau local (LAN), WAN, protocoles de communication, bande passante, etc.) ;
- La description des services offerts par les opérateurs télécoms pour les échanges de l'établissement de santé avec l'extérieur (liaison spécifique/internet, bande passante garantie pour les échanges, engagements en cas de panne, etc.)

7.2 PRINCIPES DE SECURITE

Cette section expose les principes de sécurité définis par l'établissement pour garantir la continuité d'activité et le retour à la normale du système d'information en cas de panne. Elle contient notamment les principes établis en matière de :

- Sécurité des serveurs ;
- Supervision et contrôles du système d'information ;
- Protection des logiciels ;
- Stockage.

L'établissement de santé pourra s'appuyer sur les termes des Contrats conclus avec les sociétés chargées de la maintenance du système d'information pour renseigner cette section.

Par ailleurs, l'établissement de santé ajoutera ici toute information sur les principes de sécurité qu'il juge pertinent d'intégrer au présent PRA.

7.2.1 Sécurité des serveurs

Les informations suivantes sur la sécurité des serveurs seront notamment indiquées :

- Le nombre et la description des serveurs (serveurs physiques / virtuels) ;
- Le cas échéant, la description de la plateforme gérant les serveurs virtuels ;
- La périodicité de réplication des serveurs du centre de production vers ceux du centre de secours ;
- Les modalités de reprise de l'activité d'un serveur en cas de panne ;
- La disponibilité des applications en cas de panne d'un serveur prévue par le Contrat conclu avec la société chargée de la maintenance du SI le cas échéant ;
- La procédure de bascule des serveurs et applications actifs du site de production vers le site de secours.

7.2.2 Supervision et contrôle

Les informations suivantes sur les procédures de supervision et de contrôle du système d'information de l'établissement seront notamment indiquées :

- Les acteurs responsables de la surveillance du système (établissement, société de maintenance, ...) ;
- La description du système d'alertes mis en place en cas de dysfonctionnements ;
- Les modalités de remontées de ces alertes auprès des acteurs concernés ;
- Les horaires d'astreintes du support de supervision et de contrôle.

7.2.3 Protection logicielle

Les informations suivantes sur les protections installées afin de protéger l'infrastructure technique de l'établissement seront notamment indiquées :

- La protection des serveurs : mise à jour des OS, protections contre les logiciels malveillants, … ;
- La protection des postes de travail : mise à jour des OS, protections contre les logiciels malveillants, … ;
- La protection de la messagerie : logiciel anti-spam, vérification des emails entrants et sortants, ...

7.2.4 Stockage

Cette section présente les principes de stockage des serveurs et des documents bureautiques créés par les utilisateurs du système d'information de l'établissement de santé.

7.3 LES ENVIRONNEMENTS

Cette section présente les environnements – de production, de test, de formation – dont dispose l'établissement de santé. Les informations suivantes seront notamment indiquées :

- L'existence ou non d'environnements par application (production, test, formation) ;
- Les règles d'accès à ces environnements (carte, codes d'accès, …) ;

- Les principes de test et de formation des utilisateurs à une nouvelle application sur ces environnements.

L'établissement de santé pourra ajouter ici toute information sur les environnements qu'il juge pertinent d'intégrer dans le présent PRA.

Dans le cadre de l'élaboration de son PRA du système d'information, l'établissement de santé pourra notamment s'appuyer sur les documents suivants :

- CARTOU Cédric ; La sécurité du système d'information des établissements de santé ; Presses de l'EHESP ; 2012 ;
- Club de la Sécurité de l'Information Français (CLUSIF) ; Plan de continuité d'activité - Stratégie et solutions de secours du SI ; Septembre 2003 ;
- AFNOR Normalisation ; Plan de continuité d'Activité pour les PME/PMI de la région Centre – outil méthodologique ; 2010

3.4 FICHE PRATIQUE 4 : EXEMPLE DE MÉTHODE D'ÉVALUATION DES TAUX DE DISPONIBILITÉ DES APPLICATIONS

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Fiabilité, disponibilité » comprend 3 indicateurs, dont l'indicateur P2.2 portant sur **la définition d'un taux de disponibilité cible des applicatifs et mise en œuvre d'une évaluation de ce taux[10].**

Dans le cadre de l'outillage des établissements de santé pour l'atteinte des pré-requis du programme Hôpital numérique, la DGOS met à la disposition des établissements une fiche pratique proposant une méthode d'évaluation du taux de disponibilité.

PRESENTATION DE LA FICHE PRATIQUE

L'élaboration de la cartographie applicative du SIH s'accompagne de l'évaluation des besoins en disponibilité. Il convient donc, une fois les taux de disponibilité cibles définis, d'être en capacité de les mesurer.

Le présent document présente un exemple de méthode d'évaluation des taux de disponibilité des applications.

[10] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

1. LE BESOIN EN DISPONIBILITE DES APPLICATIONS

Ce paragraphe est basé sur les travaux menés dans le cadre de l'élaboration de la Politique Générale de sécurité du Système d'Information de Santé, travaux menés par l'ASIP Santé et piloté par la DSSIS.

La disponibilité est l'aptitude d'un dispositif à être en état de fonctionner dans des conditions données. C'est la disponibilité opérationnelle des applications dont il s'agit ici, pour fournir aux utilisateurs le service attendu.

Les besoins en disponibilité sont évalués en fonction de la criticité de l'application, c'est-à-dire en matière de risques et en matière de qualité/sécurité de la prise en charge des patients. Cette évaluation doit être faite par chaque établissement en prenant l'avis des utilisateurs des différentes applications. Dans le cas où les services de l'établissement expriment des besoins de disponibilité différents pour une même application, c'est le besoin en disponibilité le plus élevé qui est retenu.

Une échelle de 1 à 4 permet de classifier les applications selon leur besoin en disponibilité :

1	Faible	Absence de besoin de disponibilité. L'application peut être indisponible sans limite
2	Significatif	L'application peut être indisponible pendant une durée importante mais limitée.
3	Important	L'application peut être indisponible pendant une courte durée.
4	Critique	L'application ne doit pas être indisponible.

Les besoins en disponibilité sont valorisés comme suit (selon les travaux menés dans le cadre de la PGSSI-S) :

1. Faible : taux de disponibilité supérieur à 95 % ce qui correspond à une durée d'indisponibilité de 36h par mois ou de 18j par an
2. Significatif : taux de disponibilité supérieur à 99% ce qui correspond à une durée d'indisponibilité de 7h par mois ou de 3,5j par an
3. Important : taux de disponibilité supérieur à 99,5% ce qui correspond à une durée d'indisponibilité de 3h30 par mois ou de 2j par an
4. Critique : taux de disponibilité supérieur à 99,9% ce qui correspond à une durée d'indisponibilité de 40 min par mois ou de 8h30 par an

2. LE TAUX DE DISPONIBILITE DES APPLICATIONS

Pour évaluer la disponibilité réelle des applications, il faut pour chacune d'elles, mesurer les temps de non disponibilité, en distinguant les indisponibilités programmées et les pannes.

En cas d'indisponibilité programmée ou non programmée, le temps d'indisponibilité correspond à la durée totale entre l'arrêt et la remise à disposition de l'application.

Le taux d'indisponibilité est calculé (avec une approximation suffisante) à partir de la formule suivante :

- **Disponibilité = (1 – temps d'indisponibilité / temps de la mesure) x 100%**

Les temps d'indisponibilité doivent être de même unité (si l'unité est la minute, les temps d'indisponibilité et de mesure doivent être mesurés en minutes).

Ce taux de disponibilité est calculé pour chaque application critique.

Une médiane des différents taux est calculé pour répondre aux pré-requis du Programme Hôpital Numérique.

3. METHODE D'EVALUATION DU TAUX DE DISPONIBILITE

Le programme Hôpital numérique n'impose pas de méthode d'évaluation du taux de disponibilité d'une application. Dans cette fiche, il est proposé un moyen simple pouvant être adopté par l'établissement.

Il existe plusieurs façons de définir et de mesurer le taux de disponibilité ; soit on mesure le fonctionnement de l'application sur les serveurs, soit on mesure que l'application est utilisable sur le poste de travail ; la dernière mesure prend en compte les pannes de réseau, de poste de travail. Dans le cadre des pré-requis du programme Hôpital numérique, il est proposé une mesure simple faite au niveau des serveurs de l'établissement.

La mise en œuvre d'un outil de supervision au niveau des serveurs suffit : il peut permettre de réaliser un calcul automatique des temps d'indisponibilité et de relever *a* minima :

- La date et l'heure de l'incident ou de l'arrêt programmé ;
- L'application concernée ;
- La date et l'heure de retour à la normale.

En cas d'absence d'outil de supervision système, ces temps pourront être calculés de manière manuelle par une personne habilitée. Une procédure sera alors élaborée afin de décrire le processus de mesure manuelle des temps d'indisponibilité.

Cette traçabilité est effectuée au fil de l'eau, pour chaque incident et arrêt programmé qui se produit. Le taux de disponibilité est évalué de façon régulière à partir de ces données, pour chaque application, selon la formule présentée précédemment. Le suivi de l'indicateur permet de détecter des dérives ou de mesurer les progrès de disponibilité.

Le taux de disponibilité des applicatifs est calculé en faisant la médiane des taux par application.

Il est évalué à fréquence régulière, par mois ou par trimestre par exemple.

4. ANNEXE : EXEMPLES DE BESOIN EN DISPONIBILITE POUR DES APPLICATIONS

1 - Besoin faible

- Base de données codées pour calculs statistiques
- Photos destinées à l'illustration des dossiers et à l'enseignement

2 - Besoin significatif

- Liste des essais cliniques, études et projets
- Gestion des échantillons biologiques
- Système de commande de repas
- Check-list opératoire

3 - Besoin important

- Accès au SGL (Système de Gestion de laboratoire) pour consulter un résultat d'analyses (si indisponible, possibilité de récupérer les résultats directement à partir des automates)
- Accès au PACS pour comparaison examens antérieurs à des fins d'interprétation (possibilité de différer l'interprétation)
- Accès au système de gestion des rendez-vous (possibilité d'interrompre temporairement la prise de rendez-vous)
- Worklists pour modalités d'imagerie

4 - Besoin critique

- Accès aux images radiologiques (via le PACS) et aux consultations préopératoires et pré-anesthésiques en contexte d'intervention en bloc opératoire
- Accès à la carte de groupe et aux RAI (Recherche d'Agglutinines Irrégulières) avant un acte transfusionnel
- Accès aux dernières prescriptions et administrations dans une unité d'hospitalisation (risque d'erreur de médication : de double prescription ou administration, risque d'absence d'administration)
- Accès au serveur d'identité pour la création d'un nouveau dossier patient
- Accès aux transmissions infirmières

3.5 FICHE PRATIQUE 5 : BONNES PRATIQUES D'ÉLABORATION DES PROCÉDURES DE FONCTIONNEMENT EN MODE DÉGRADÉ / DE RETOUR À LA NORMALE DU SYSTÈME D'INFORMATION

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Fiabilité, disponibilité » comprend 3 indicateurs, dont l'indicateur P2.3 portant sur **l'existence de procédures assurant d'une part un fonctionnement dégradé du système d'information au cœur du processus de soins en cas de panne et d'autre part un retour à la normale**[11].

Dans le cadre de l'outillage des établissements de santé pour l'atteinte des pré-requis du programme Hôpital numérique, la DGOS met à la disposition des établissements une fiche pratique détaillant la méthode d'élaboration de ces procédures.

PRESENTATION DE LA FICHE PRATIQUE

Le présent document présente des bonnes pratiques d'élaboration des procédures de fonctionnement en mode dégradé et de retour à la normale du système d'information.

Chaque service ou entité qui utilise des applications logicielles « métier » critiques doit pouvoir continuer à travailler en l'absence de ces applications.

[11] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

Ce document présente la démarche et les questions à se poser pour élaborer une procédure de fonctionnement en mode dégradé. Il propose également quelques exemples.

Par fonctionnement en mode dégradé, nous entendons :

- La bascule du mode de fonctionnement nominal vers le mode dégradé ;
- Le fonctionnement en mode dégradé durant la durée d'indisponibilité du système ;
- Le retour au fonctionnement nominal une fois le système disponible.

1. DEMARCHE D'ELABORATION DES PROCEDURES

Cette démarche est à faire globalement en impliquant chaque service ou entité qui utilise des applications métier critiques pour assurer ses activités :

- Les unités de soins ;
- Les unités de soins critiques ;
- Le bloc opératoire ;
- Les plateaux techniques : radiologie, biologie ;
- Etc.

Elle est menée en association entre un référent des services concernés et le référent de la DSI.

En pratique, chaque service doit s'approprier les procédures dégradées définies par l'établissement, s'assurer de leur mise à jour et les adapter, le cas échéant, à ses modalités spécifiques de fonctionnement. .

1.1 LISTER LES PROCEDURES A ELABORER

A minima il faut évidemment prévoir pour chacune des applications critiques (recensées dans la cartographie applicative) une procédure pour basculer en mode dégradé, une procédure de fonctionnement en mode dégradé et une procédure pour revenir en fonctionnement normal. Pour une même application, ces procédures devraient être adaptées aux services et usages.

Pour les procédures, Il faut d'abord envisager le cas de l'arrêt programmé; il est dans ce cas, possible d'anticiper et de préparer l'arrêt et le basculement en mode dégradé. Les documents nécessaires au maintien de l'activité peuvent être imprimés avant l'arrêt. Cette tache sera d'autant moins lourde que l'arrêt programmé doit être prévu dans une période d'activité réduite (nuit, week-end).

Les procédures prévues pour le cas de l'arrêt programmé, doivent être adaptées à ce qui est possible pour les cas de pannes.

1.2 IDENTIFIER LES FONCTIONS ET LES INFORMATIONS ESSENTIELLES POUR LE SERVICE CONCERNE

Parmi toutes les fonctionnalités de l'application métier concernée, se limiter aux fonctions majeures, indispensables au maintien de l'activité, en distinguant :

- Les activités relatives aux échanges avec des services extérieurs ;

- Les activités propres au fonctionnement interne du service.

- **Activités relatives aux échanges avec les services extérieurs**

Pour une unité de soins, il s'agit d'une part de pouvoir continuer à produire des demandes (imagerie, biologie, examens complémentaires, prescription de médicaments), d'autre part de recevoir et consulter les résultats.

Pour un plateau technique, il s'agit de recevoir les prescriptions et demandes diverses, et pouvoir y répondre.

Recenser l'ensemble des services avec lequel le service concerné travaille et les informations échangées avec ces services, par exemple :

- L'identité du patient ;
- L'objet de la demande ;
- Le service prestataire ;
- Des informations complémentaires du patient ;
- Etc.

- **Activités propres au fonctionnement interne du service**

Pour une unité de soins, il faut par exemple pouvoir continuer à prescrire et administrer les soins et les produits de santé.

Pour un plateau technique, il faut pouvoir continuer à réaliser les examens demandés et produire les résultats, donc par exemple pour la radiologie, avoir la liste des rendez-vous et examens programmés pour la journée.

Chaque service liste les informations nécessaires à son fonctionnement, par exemple :

- Les prescriptions ;
- Le plan de soins ;
- Les rendez-vous du jour ;
- Etc.

1.3 METTRE EN ŒUVRE LES MOYENS TECHNIQUES POUR MAINTENIR LES ACTIVITES

Une fois identifiées les informations indispensables à la poursuite des activités, il s'agit de préciser et définir :

- Les documents et modèles à utiliser ;
- Comment trouver ces documents en l'absence de l'application informatique

Pour ce faire, il conviendra de tenir compte des logiciels associés aux dispositifs médicaux susceptibles de détenir ces informations.

Pour mettre en œuvre ces moyens, il faut s'appuyer sur les solutions proposées par les éditeurs des applications informatiques et bâtir la procédure à mettre en œuvre avec son support. Souvent, les solutions et procédures sont différentes pour les arrêts programmés et pour les pannes ; tout arrêt programmé d'une application critique doit faire l'objet d'une proposition de fonctionnement en mode dégradé par l'éditeur ou l'intégrateur.

Le principe général de ces solutions est de dupliquer les informations essentielles (typiquement une synthèse du dossier patient, le plan de soins, la prescription en cours, etc.) en dehors de la base de données de l'application, sous une forme directement imprimable

(par exemple des pdf.). Cette extraction des données sous un format imprimable, peut être faite à une fréquence adaptée aux besoins ; les données sont alors stockées sur un serveur central ou des postes locaux dans les services (cette étape peut nécessiter un paramétrage spécifique à réaliser dans l'application, avec le support de l'éditeur (paramétrage des traitements batch, réalisation des modèles de documents à imprimer, etc.). Il faut veiller à la confidentialité des informations contenues dans ces postes.

Il faut ensuite prévoir les procédures pour imprimer les supports en cas d'arrêt programmé ou de panne pour assurer le fonctionnement en mode dégradé ; la diffusion des documents aux utilisateurs est à prévoir.

Pour d'autres cas, des moyens simples doivent être prévus, souvent en s'appuyant sur les suggestions des utilisateurs, comme par exemple l'impression de bordereaux vierges (par exemple, aux admissions, ou pour les demandes d'examens des unités de soins) conservés dans les services.

1.4 DEFINIR LE MODE DE BASCULE DU FONCTIONNEMENT NOMINAL VERS LE FONCTIONNEMENT EN MODE DEGRADE

Une fois les moyens « techniques » préparés qui permettent d'assurer le fonctionnement en mode dégradé, il est nécessaire de préciser les procédures de bascule en mode dégradé, en continuant à distinguer les arrêts programmés et les pannes.

En effet en cas d'arrêt programmé (typiquement pour une mise à jour de version), la direction et le personnel sont informés à l'avance; en particulier, la durée prévisionnelle de l'arrêt est indiquée (sur la base des informations fournies par l'industriel réalisant la maintenance); les informations et documents nécessaires sont imprimés avant l'arrêt de l'application de façon à ce qu'ils soient déjà disponibles dans le service au moment de l'arrêt. Les arrêts programmés sont prévus à des moments de plus faible activité; le volume d'informations à imprimer est de ce fait réduit.

En cas de panne, les mêmes documents sont imprimés, autant qu'il est possible avec les moyens disponibles, et transmis aux utilisateurs. Informer la direction et les utilisateurs doit être prévu.

1.5 DEFINIR LE MODE DE RETOUR AU FONCTIONNEMENT NOMINAL

La procédure de fonctionnement en mode dégradé doit prévoir le retour à la normale.

Durant la période de fonctionnement en mode dégradé des informations ont été produites principalement sur des documents papiers.

Une fois le système de nouveau disponible, il est nécessaire de reprendre manuellement dans le système les informations, pour que l'application soit de nouveau à jour. Il faut donc conserver les documents utilisés et définir quelles sont les données à reprendre et par qui. Il est nécessaire de prendre en compte le temps total de perte de données qui peut être supérieur au temps de l'arrêt lorsque les données sont restaurées à partir de la sauvegarde.

2. EXEMPLES DE PROCEDURES

Pour une unité de soins :

- **En fonctionnement normal**
  - Un correspondant de la DSI est identifié pour préparer le fonctionnement en mode dégradé et faciliter le basculement (par exemple, il s'assure de la disponibilité des documents nécessaires au fonctionnement en mode dégradé) ;
  - Avoir en anticipation, dans les services, à disposition les différents bordereaux vierges de demandes nécessaires aux échanges avec les autres services ;
  - Informer de l'existence de cette procédure et la tenir à disposition dans le service.

- **Fonctionnement en mode dégradé**
  - Information des personnels (du service et des services extérieurs) que la procédure de fonctionnement en mode dégradé s'applique
  - Utilisation des supports prévus et mise en œuvre de l'organisation prévue
  - Impression des documents pdf. stockés sur le serveur centralisé
  - Diffusion des documents vers les utilisateurs concernés

- **Retour à la normale**
  - Information des personnels (du service et des services extérieurs)
  - Identification des données « perdues » (*en cas de restauration des données à partir des données de sauvegarde, il peut y avoir eu perte de données, entre la date de la dernière sauvegarde et le moment où la procédure en mode dégradé a été appliquée)*
  - Collecte des informations à reprendre dans le système
  - Saisie des informations dans le système

3. POUR ALLER PLUS LOIN

Dans le cadre de l'élaboration des procédures de fonctionnement en mode dégradé et de retour à la normale du système d'information, l'établissement de santé pourra notamment s'appuyer sur le document suivant :

- CARTOU Cédric ; La sécurité du système d'information des établissements de santé ; Presses de l'EHESP ; 2012 ;

3.6 FICHE PRATIQUE 6 : FICHE DE POSTE TYPE D'UN RSSI ET DESCRIPTION DES FONCTIONS D'UN RÉFÉRENT SÉCURITÉ DU SYSTÈME D'INFORMATION

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Confidentialité » comprend 5 indicateurs, dont l'indicateur P3.1 portant sur **l'existence d'une politique de sécurité formalisée pour les applications au cœur du processus de soins et fondée sur une analyse des risques au sein de l'établissement ; existence d'une fonction de référent sécurité**[12].

Dans le cadre de l'outillage des établissements de santé pour l'atteinte des pré-requis du programme Hôpital numérique, la DGOS met à la disposition des établissements la présente fiche pratique qui propose une fiche de poste type d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) et décrit les fonctions d'un référent sécurité du système d'information

PRESENTATION DE LA FICHE PRATIQUE

Cette fiche pratique a pour objectifs de présenter les fonctions relevant du RSSI d'un établissement de santé, ainsi que les compétences techniques et personnelles requises pour les accomplir. Le RSSI peut-être mutualisé entre plusieurs structures.

La fiche de poste du RSSI élaborée par l'établissement de santé précise *a minima* les informations suivantes :

1. La présentation de l'établissement de santé / du service de rattachement du RSSI ;
2. Le contexte d'intervention du RSSI ;

[12] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

3. La description des missions et des activités du RSSI ;
4. Le profil et les compétences attendues pour occuper cette fonction ;
5. Les moyens mis à disposition du RSSI par l'établissement de santé.

Pour accompagner les établissements de santé dans **l'élaboration d'une fiche de poste du RSSI** (à partir de la présente fiche pratique) adaptée à leurs besoins sont distingués ci-après dans le document par un code couleur :

- En violet, sont précisées des explications sur l'objet et le contenu d'une section, ainsi que des informations ayant vocation à accompagner l'établissement dans l'élaboration de la fiche de poste du RSSI. Ces indications devront être supprimées de la fiche avant sa diffusion au sein de l'établissement.

- **En noir sont indiquées les listes a maxima des missions / activités pouvant être exercées par le RSSI d'un établissement et les compétences attendues à ce poste. Parmi ces listes, chaque structure sélectionne celles qu'il conserve in fine dans la fiche de poste du RSSI au regard de ses besoins propres.**

A défaut de pouvoir disposer d'un RSSI au sein de sa structure, l'établissement de santé nommera un référent sécurité dans le cadre de l'atteinte du pré-requis 3.1 du programme Hôpital numérique[13]. Ce référent sécurité aura notamment pour fonction de :

- S'assurer que la Politique de sécurité des systèmes d'information de l'établissement de santé est définie et validée par la Direction Générale, testée et mise à jour *a minima* tous les trois ans au sein de la structure ;
- Veiller à ce qu'une analyse des risques de la sécurité des systèmes d'information ait été menée au sein de l'établissement ;
- Mettre en œuvre la Politique de sécurité des systèmes d'information définie au sein de l'établissement de santé ;
- Auditer et contrôler l'application des règles de la Politique de sécurité des systèmes d'information au sein l'établissement et, le cas échéant, d'alerter la Direction générale en cas de défaut d'application de cette Politique.

[13] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

Identification du poste	RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION

1. PRESENTATION DE L'ETABLISSEMENT DE SANTE / DU SERVICE DE RATTACHEMENT DU RSSI

Cette section vise à décrire les caractéristiques de l'établissement de santé et du service au sein duquel le RSSI exerce ses missions.

Les informations suivantes sont notamment décrites :

- Les missions, l'organisation et la composition de l'établissement et du service auquel est rattaché le RSSI ;
- La place du RSSI dans l'organigramme, son positionnement hiérarchique et les liens fonctionnels le rattachant aux autres acteurs de l'établissement de santé.

L'établissement de santé peut également ajouter toute autre information sur son organisation qu'il juge pertinent de porter à la connaissance du RSSI.

2. CONTEXTE D'INTERVENTION

Cette section a pour objectif de dire s'il s'agit d'une création de poste ou d'un remplacement. Dans ce dernier cas, il convient de décrire le niveau de maturité de l'établissement en matière de sécurité de son système d'information et les actions déjà entreprises dans ce domaine.

Par exemple, les informations suivantes peuvent être indiquées :

- L'existence d'une Politique de sécurité des systèmes d'information, d'un plan de continuité d'activité, ... ;
- L'historique des analyses de risques et des audits de sécurité des systèmes d'information réalisées ;
- Les actions de sensibilisation des acteurs de l'établissement à la sécurité des systèmes d'information menées.

L'établissement peut ajouter toute autre information sur le contexte d'intervention qu'il juge pertinent de porter à la connaissance du RSSI.

L'établissement précise également si le poste est à temps complet dans l'établissement de santé ou partagé (mutualisé) entre plusieurs structures.

3. DESCRIPTION DES MISSIONS ET DES ACTIVITES

La présente section vise à décrire les missions et les activités placées sous la responsabilité du RSSI. La liste proposée ci-dessous recense ainsi *a maxima* ces missions et activités. L'établissement de santé ne conservera que celles qu'il souhaite confier au RSSI en fonction de ses propres besoins.

Le Responsable de la sécurité des systèmes d'information de l'établissement de santé est chargé de réaliser les missions et les activités suivantes :

- **Définition et mise en œuvre de la Politique de sécurité des systèmes d'information :**

- Définit les objectifs et les besoins liés à la sécurité des systèmes d'information de l'établissement, en collaboration avec les acteurs concernés (direction générale, direction des systèmes d'information, direction des ressources humaines, direction qualité, représentants du personnel médical et soignant) ;
- Rédige la Politique de sécurité des systèmes d'information et les procédures de sécurité associées en collaboration avec les acteurs concernés (cf. ci-dessus) ;
- Met en œuvre la Politique de sécurité des systèmes d'information au sein de l'établissement de santé, en assure les évolutions et les mises à jour ;
- Met en place une organisation permettant d'assurer, dans la durée, la gouvernance de la sécurité du système d'information de l'établissement ;

- **Diagnostic et analyse des risques de la sécurité des systèmes d'information :**
  - Choisit une méthode d'analyse de risques adaptée à la taille et à l'activité de l'établissement ;
  - Evalue les risques sur la sécurité des systèmes d'information ;

- **Choix des mesures de sécurité et plan de mise en œuvre :**
  - Etudie les moyens permettant d'assurer la sécurité des systèmes d'information et leur bonne utilisation par les acteurs de l'établissement ;
  - Propose à la direction pour arbitrage une liste de mesures de sécurité à mettre en œuvre, assure dans la durée, le suivi et l'évolution de ce plan d'actions ;
  - Assure la maîtrise d'ouvrage de la mise en œuvre des mesures de sécurité (cette mission, selon que le type de mesure soit technique soit organisationnelle, peut être éventuellement partagée avec un responsable métier ou le responsable du système d'information) ;

- **Sensibilisation, formation et conseil sur les enjeux de la sécurité des systèmes d'information :**
  - Informe régulièrement et sensibilise la Direction générale de l'établissement sur les enjeux et les risques de la sécurité des systèmes d'information ;
  - Conduit des actions de sensibilisation et de formation auprès des utilisateurs sur les enjeux de la sécurité des systèmes d'information ;
  - Participe à la réalisation de la charte de sécurité des systèmes d'information de l'établissement, et en assure la promotion auprès de l'ensemble des utilisateurs ;

- **Audit et contrôle de l'application des règles de la Politique de sécurité des systèmes d'information :**
  - Conduit régulièrement des audits de sécurité des systèmes d'information afin de vérifier la bonne application de la Politique de sécurité par les acteurs de l'établissement ;
  - Surveille et gère les incidents de sécurité survenus au sein de l'établissement ;
  - Vérifie l'intégration de la sécurité des systèmes d'information dans l'ensemble des projets de l'établissement de santé ;

- **Veille technologique et prospective :**
  - Suivi des évolutions réglementaires et techniques afin de garantir l'adéquation de la Politique de sécurité des systèmes d'information avec ces évolutions.

4. PROFIL ET COMPETENCES REQUISES

Cette section vise à décrire le profil requis et les compétences techniques et personnelles nécessaires pour occuper le poste du RSSI. Une liste de compétences *a maxima* est proposée ci-dessous. L'établissement ne conserve que les compétences propres à ses besoins, en lien avec les missions et les activités du RSSI décrites préalablement.

- **Niveau de formation et d'expérience :**
  - Formation de niveau licence (ou master 2) avec une spécialisation complémentaire en sécurité des systèmes d'information ;
  - Cadre technique ayant une expérience avérée dans la conduite de projets en milieu hospitalier.
- **Compétences techniques :**
  - Connaissance des concepts techniques des applications informatiques hospitalières, des réseaux informatiques et des mécanismes de sécurité ;
  - Connaissance des standards de sécurité ISO 2700x ;
  - Expérience dans le pilotage de projets organisationnels dans le milieu hospitalier ;
  - Connaissance juridique sur la sécurité des systèmes d'information, et particulièrement des textes régulant la santé ;
  - Notions sur la réglementation et les procédures des marchés publics (pour les établissements publics).
- **Compétences personnelles :**
  - Capacité à piloter et gérer des projets ;
  - Capacité à organiser et conduire le changement ;
  - Capacité à gérer des situations de crise ;
  - Capacité à animer des groupes de travail, sessions de sensibilisation et formation,
  - Bon relationnel et esprit de synthèse.

5. MOYENS MIS A DISPOSITION

Cette section précise les moyens humains, matériels et financiers qui seront mis à la disposition du RSSI pour mener à bien les missions et les activités décrites précédemment (exemples : poste de travail, équipe dédiée, budget alloué, ...).

3.7 FICHE PRATIQUE 7 : CHARTE TYPE D'ACCÈS ET D'USAGE DU SYSTÈME D'INFORMATION

CONTEXTE DE LA FICHE PRATIQUE

Le socle commun du programme Hôpital numérique est constitué :

- **De 3 pré-requis** indispensables pour assurer une prise en charge du patient en toute sécurité.
  - Identités, mouvements ;
  - Fiabilité – disponibilité ;
  - Confidentialité.
- **De 5 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.
  - Les résultats d'imagerie, de biologie et d'anapath ;
  - Le dossier patient informatisé et interopérable ;
  - La prescription électronique alimentant le plan de soins ;
  - La programmation des ressources et l'agenda du patient ;
  - Le pilotage médico-économique.

Le pré-requis « Confidentialité » comprend 5 indicateurs, dont l'indicateur P3.2 portant sur **l'existence d'une charte ou d'un document formalisant les règles d'accès et d'usage du système d'information, en particulier pour les applications gérant des informations de santé à caractère personnel, diffusé au personnel, aux nouveaux arrivants, prestataires et fournisseurs**[14]**, ainsi qu'aux instances représentatives du personnel**.

Dans le cadre de l'outillage des établissements de santé par la DGOS pour l'atteinte des pré-requis du programme Hôpital numérique, la présente fiche pratique portant sur **la Charte d'accès et d'usage du système d'information** est mise à la disposition des établissements de santé.

PRESENTATION DE LA FICHE PRATIQUE

La présente Charte type a pour objectif de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet d'un établissement de santé et rappelle aux utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information, conformément à la politique de sécurité des systèmes d'information définie par l'établissement de santé. L'établissement de santé veillera à présenter la Charte aux instances décisionnaires et à en assurer la publicité maximale auprès des utilisateurs.

Pour accompagner les établissements dans **l'élaboration d'une Charte d'accès et d'usage du système d'information** (à partir de la présente fiche pratique) adaptée à leur contexte et leur organisation sont distingués ci-après dans le document par un code couleur :

[14] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html*

- En violet encadré, des explications sur l'objet et le contenu d'une section, ainsi que des informations ayant vocation à accompagner l'établissement dans l'élaboration de sa propre Charte. Ces indications doivent être supprimées de la Charte avant sa diffusion au sein de l'établissement.

- En bordeaux, des informations propres à chaque structure. Ces informations doivent donc être renseignées et contextualisées par l'établissement lors de l'élaboration de la Charte d'accès et d'usage du système d'information.

- **En noir, des éléments d'ordre générique qui peuvent constituer la base de la Charte d'accès et d'usage du système d'information de l'établissement ; ces éléments pouvant être modifiés / complétés par l'établissement de santé.**

1. OBJET DU DOCUMENT

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du *[indiquer le nom de l'établissement de santé]* et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de l'établissement, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'établissement.

Cette Charte a été validée par la Direction générale de l'établissement. Préalablement, elle a été notifiée à sa mise en œuvre au Comité d'Etablissement et à la Commission médicale d'Etablissement. Elle constitue une annexe au Règlement Intérieur de l'établissement. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance. La Charte est mise à leur disposition sur l'Intranet et affichée dans les locaux de l'établissement de santé.

La Charte d'accès et d'usage du système d'information doit être validée conjointement par la Direction générale et la Commission médicale de l'établissement. Elle constitue une annexe au Règlement intérieur.

2. CHAMP D'APPLICATION

Cette section décrit le périmètre d'application de la présente Charte et précise les utilisateurs du système d'information de l'établissement qui sont concernés par celle-ci.

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du *[indiquer le nom de l'établissement de santé*], ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau ;
- Ordinateurs portables ;
- Terminaux portables ;
- Imprimantes simples ou multifonctions ;
- Tablettes ;
- Smartphones ;
- *[Ajouter toute autre ressource que la structure souhaite intégrer au périmètre de la Charte*].

Cette Charte s'applique à l'ensemble du personnel de l'établissement de santé, tous statuts confondus, et concerne notamment les agents permanents ou temporaires (stagiaires, internes, doctorants, prestataires, fournisseurs, sous-traitants, …) utilisant les moyens informatiques de l'établissement et les personnes auxquelles il est possible d'accéder au

système d'information à distance directement ou à partir du réseau administré par l'établissement.

Dans la présente Charte, sont désignés sous les termes suivants :

- **Ressources informatiques**: les moyens informatiques, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité ;
- **Outils de communication** : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses (web, messagerie, forum, etc.) ;
- **Utilisateurs** : les personnes ayant accès ou utilisant les ressources informatiques et les services internet de l'établissement.

3. CADRE REGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- Le traitement numérique des données, et plus précisément :
  - Le traitement de données à caractère personnel et le respect de la vie privée ;
  - Le traitement de données personnelles de santé ;
- Le droit d'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données médicales ;
- Le secret professionnel et le secret médical ;
- La signature électronique des documents;
- Le secret des correspondances ;
- La lutte contre la cybercriminalité ;
- La protection des logiciels et des bases de données et le droit d'auteur.

La présente Charte d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

4. CRITERES FONDAMENTAUX DE LA SECURITE

4.1 PRINCIPES

L'établissement de santé héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médico-techniques, …), et sur les personnels (paie, gestion du temps, évaluations, accès à Internet et à la messagerie, …).
L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images),

transmise par des réseaux informatiques privés ou internet, par la poste, oralement et/ou par téléphone,...
La **sécurité de l'information** est caractérisée comme étant la préservation de :

- **Sa disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin;
- **Son intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie ;
- **Sa confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder ;
- **Sa traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

4.2 UNE MISSION SECURITE

[Indiquer le nom de la direction / département de l'établissement en charge des systèmes d'information] fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de l'établissement en s'assurant que ces moyens sont bien au service de la production de soins. Elle doit donc définir et empêcher les abus.

4.3 UN ENJEU TECHNIQUE ET ORGANISATIONNEL

Les enjeux majeurs de la sécurité sont la qualité et la continuité des soins, le respect du cadre juridique sur l'usage des données personnelles de santé.

Pour cela, *[indiquer le nom de la direction / département de l'établissement en charge des systèmes d'information*] déploie un ensemble de dispositifs techniques mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut-être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

4.4 UNE GESTION DES RISQUES

L'information médicale, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des patients. Une information manquante, altérée ou indisponible peut constituer une perte de chance pour le patient (exemples : erreur dans l'identification d'un patient (homonymie par exemple), perte de données suite à une erreur d'utilisation d'une application informatique, …). La sécurité repose sur une gestion des risques avec des analyses des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion. La présente Charte d'accès et d'usage du système d'information s'inscrit dans ce plan de communication.

5. REGLES DE SECURITE

Cette section présente les règles de sécurité du système d'information définies par l'établissement de santé. Il décrit notamment les dispositions relatives à :
- L'obligation de discrétion et de confidentialité ;
- La protection de l'information ;
- L'usage des comptes et des mots de passe ;
- L'usage des outils de communication (Internet, messagerie, téléphone et fax, …) ;
- La préservation de l'image de marque de l'établissement ;

Afin de répondre au pré-requis du programme Hôpital numérique, la Charte d'accès et d'usage du système d'information de l'établissement de santé devra préciser les règles d'accès au dossier patient informatisé par les professionnels habilités, notamment d'accès aux données issues de consultations ou d'hospitalisations[15]. Il est recommandé que l'accès à ces données par les professionnels habilités se fasse par le biais d'un login et d'un mot de passe individuel robuste et renouvelé à un rythme régulier par l'utilisateur.

L'établissement de santé adaptera cette section aux règles de sécurité qu'il souhaite mettre en place au sein de sa structure dans le respect de la législation en vigueur et des droits et libertés reconnus aux utilisateurs.

Il pourra enfin être ajouté toute information relative aux règles de sécurité que l'établissement de santé juge pertinente de porter à la connaissance des utilisateurs (exemples : mode d'obtention d'un droit d'accès aux systèmes informatiques, modalités de fermeture d'un accès au réseau en cas de départ ou de changement d'affectation / d'absence de longue durée, …).

L'accès au système d'information de l'établissement est soumis à autorisation. Une demande préalable écrite est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; la demande exprimée par l'utilisateur est au préalable validée par son manager, qui précise les accès nécessaires à son collaborateur et la transmet par écrit *[indiquer le nom de la direction / département de l'établissement en charge des systèmes d'information*].

Le service informatique attribue alors au demandeur son droit d'accès et lui communique la présente Charte d'accès et d'usage du système d'information. Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cession, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect des dispositions de la présente Charte par l'utilisateur.

L'obtention d'un droit d'accès au système d'information de l'établissement de santé entraîne pour l'utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous.

[15] *DGOS ; Guide des indicateurs des pré-requis et des domaines prioritaires du socle commun ; disponible à l'adresse suivante : http://www.sante.gouv.fr/programme-hopital-numerique.html ; Indicateur P3.2 Existence d'une charte ou d'un document formalisant les règles d'accès et d'usage du système d'information, en particulier pour les application gérant des informations de santé à caractère personnel, diffusé au personnel, aux nouveaux arrivants, prestataires et fournisseurs.*

5.1 CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION

Les personnels de l'établissement sont soumis au secret professionnel et/ou médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'accès aux donnes de santé à caractère personnel des patients par des professionnels habilités se fait avec une carte CPS.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

5.2 PROTECTION DE L'INFORMATION

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important de ne stocker aucune donnée ni aucun document sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées sur des serveurs centraux implantés dans des salles protégées. De même, les documents bureautiques produits doivent être stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smart phone, …) ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue d'un voisin de train … ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, disquette, clé, disque dur, …). Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les medias de stockage amovibles (exemples : clefs USB, CD-ROM, disques durs …) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit être fait avec une très grande vigilance. L'établissement se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaitrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement.

5.3 USAGE DES RESSOURCES INFORMATIQUES

Seules des personnes habilitées de l'établissement de santé (ou par son intermédiaire la société avec laquelle il a contracté) ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'établissement et plus globalement d'installer de nouveaux matériels informatiques.

L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux, …) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées de l'établissement (ou par son intermédiaire la société avec laquelle il a contracté).

Les logiciels commerciaux acquis par l'établissement ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'établissement.

Le cas échéant, l'établissement de santé ajoutera également ici les règles de sécurité qu'il aura définies en matière d'usage par le personnel hospitalier d'équipements personnels (« Bring your Own Devices (BYOD) »), de type tablette, smart phone, etc.

5.4 USAGE DES OUTILS DE COMMUNICATION

Les outils de communication tels que le téléphone, le fax, Internet ou la messagerie sont destinés à un usage exclusivement professionnel. L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il soit très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à l'image de marque de l'établissement de santé. Il ne doit en aucun cas être porté à la vue des patients ou de visiteurs et accompagnants.

- **Usage du téléphone et du fax**

Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax n'est pas garantie.

Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après avoir vérifié l''identité de l'interlocuteur téléphonique. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires de patients ou professionnels.

La communication d'informations médicales (exemples : résultats d'examens, …) aux patients et aux professionnels extérieurs est strictement réglementée. Les utilisateurs concernés doivent se conformer à la réglementation et aux procédures de l'établissement en vigueur.

- **Usage d'Internet**

L'accès à l'Internet a pour objectif d'aider les personnels à trouver des informations nécessaires à leur mission usuelle, ou dans le cadre de projets spécifiques.

Il est rappelé aux utilisateurs que, lorsqu'ils « naviguent » sur l'Internet, leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et à ne pas mettre en danger l'image ou les intérêts de l'établissement de santé.

Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur, …) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est interdit de participer à des forums, blogs et groupes de discussion à des fins non professionnelles, et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraire à l'ordre public.

Tous les accès Internet sont tracés et enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque salarié, le détail de son activité sur l'Internet.

Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment des sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.

- **Usage de la messagerie**

L'usage de la messagerie est autorisé à l'ensemble du personnel. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement

Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre l'hôpital et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « privé » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

L'usage des listes de diffusion doit être strictement professionnel.

Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou de porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'ils transmettent par email.

Afin de ne pas surcharger les serveurs de messagerie, les utilisateurs doivent veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées. Il est rappelé que le réseau Internet n'est pas un moyen de transport sécurisé. Il ne doit donc pas servir à l'échange d'informations médicales nominatives en clair. En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes.

Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.

5.5 USAGE DES LOGIN ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENT)

Chaque utilisateur dispose de compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. Il est strictement interdit d'usurper une identité en utilisant ou en tentant d'utiliser le compte d'un autre utilisateur ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur soit dispose d'un login et d'un mot de passe, soit utilise une carte CPS ou équivalent (avec un code personnel à 4 chiffres)

Le mot de passe choisi doit être robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé tous les 6 mois. Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en charge de la sécurité des systèmes d'information, même pour une situation temporaire.

Chaque utilisateur est responsable de son compte et son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage. La plupart des systèmes informatiques et des applications de l'établissement assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications médicales et médico-techniques, les applications administratives, le réseau, la messagerie, l'Internet, … Il est ainsi possible pour l'établissement de vérifier *a posteriori* l'identité de l'utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste. Il ne faut jamais se connecter sur plusieurs postes à la fois. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le soir..

Il est interdit de contourner ou de tenter de contourner les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors de formations ou dans les manuels et procédures remis aux utilisateurs.

L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

5.6 IMAGE DE MARQUE DE L'ETABLISSEMENT

Les utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de l'établissement en utilisant des moyens, que ce soit en interne ou en externe, à travers des communications d'informations à l'extérieur de l'établissement ou du fait de leurs accès à Internet.

6. INFORMATIQUE ET LIBERTES

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du

Correspondant Informatique et Libertés (CIL) de l'établissement de santé, à défaut le Responsable de la Sécurité du Système d'Information (RSSI), qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le CIL procède ensuite aux opérations de déclaration et d'information réglementaires.

Il est rappelé que l'absence de déclaration de fichiers comportant des données à caractère personnel est passible de sanctions financières et de peines d'emprisonnement.

En cas de non-respect des obligations relatives à la loi Informatique et Libertés, le CIL serait informé et pourrait prendre toute mesure temporaire de nature à mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

7. SURVEILLANCE DU SYSTEME D'INFORMATION

Cette section décrit le dispositif de surveillance du système d'information mis en œuvre par l'établissement de santé, et notamment les modalités de contrôle de l'usage du système d'information par les utilisateurs et la gestion des traces. Il convient ainsi d'adapter cette section aux modalités de surveillance du système d'information déjà mises en place au sein de l'établissement.

7.1 CONTROLE

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

7.2 TRAÇABILITE

[Indiquer le nom de la direction / département de l'établissement en charge des systèmes d'information] assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il est accédé ;
- Le type d'opération réalisée
- Les informations ajoutées, modifiées ou supprimée des bases de données en réseau et/ ou des applications de l'hôpital ;
- La durée de la connexion (notamment pour l'accès Internet) ;

– *[Ajouter toute autre trace que le dispositif de surveillance permet d'enregistrer].*

Le personnel de la Direction du système d'information respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction, mais peuvent être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

7.3 ALERTES

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé au Responsable de la Sécurité du Système d'Information.

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les patients bénéficient d'une prise en charge sécurisée et que leur vie privée ainsi que celle des personnels soient respectées.

8. RESPONSABILITES ET SANCTIONS

Cette section présente les sanctions encourues par les utilisateurs du système d'information de l'établissement en cas de non respect des dispositions prévues par la présente Charte. L'établissement de santé adaptera ainsi cette section à la politique de sanctions en vigueur au sein de sa structure.

Les règles définies dans la présente Charte ont été fixées par la Direction générale de l'établissement de santé dans le respect des dispositions législatives et réglementaires applicables (CNIL, ASIP Santé, ...).

L'établissement ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrites dans la Charte. En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions pouvant être :

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, des moyens informatiques ;
- Un licenciement et éventuellement des actions civiles ou pénales, selon la gravité du manquement.
- *[Ajouter toute autre sanction que l'établissement souhaite mettre en œuvre*].

Outre ces sanctions, la Direction du *[indiquer le nom de l'établissement de santé]* est tenu de signaler toutes infractions pénales commises par son personnel au procureur de la République.

[Indiquer le nom du Direction de l'établissement de santé], **Directeur de l'établissement de santé**

Signature du Directeur de l'établissement de santé

[Indiquer le nom du Responsable de la sécurité du système d'information], **Responsable de la sécurité du système d'information de l'établissement de santé**

4. ASSISTANCE

Pour **toute question ou information complémentaire sur le programme Hôpital numérique**, vous pouvez contacter le chargé de mission SI (CMSI) de l'ARS de votre région.

La liste des CMSI et leurs coordonnées sont disponibles sur le site Internet du programme, à l'adresse suivante http://www.sante.gouv.fr/hopital-numerique.html

5. REMERCIEMENTS

La DGOS **adresse ses remerciements à l'ensemble des professionnels** ayant contribué aux travaux d'élaboration de la boite à outils pour l'atteinte des pré-requis du programme Hôpital numérique (i.e. l'outil d'autodiagnostic et de plan d'actions associé et les fiches pratiques) :

- Les **membres du groupe de travail « Mécanismes de financement »**, qui avaient œuvré à la définition des indicateurs constituant le socle commun du programme hôpital numérique (pré-requis et domaines fonctionnels prioritaires) et ont à nouveau contribué au groupe de travail pour étudier et enrichir la boite à outils préalablement à sa diffusion :
  - CHU de Rennes ;
  - CHU de Tours ;
  - CH de Châtellerault ;
  - Institut Curie ;
  - Centre Chirurgical Marie Lannelongue ;
  - Générale de Santé ;
  - ARS Basse-Normandie ;
  - ARS Haute-Normandie ;
  - ARS Nord Pas de Calais.

- Les **membres de l'équipe projet du programme, piloté par la DGOS** (représentants de la délégation à la stratégie des systèmes d'information de santé du ministère, de l'ANAP, de l'ASIP Santé et des ARS) ;

- Les **chargés de mission SI des ARS,** relais régionaux de la DGOS sur le programme Hôpital numérique, qui ont également participé à la revue de l'outil préalablement à sa diffusion ;

- Les **collèges de DSIO**, qui ont sollicité les établissements de santé afin de recueillir de leur part un maximum de documents-exemples déjà existants et afin de tester les outils :

- Les **établissements de santé** qui ont répondu à l'appel des collèges des DSIO et ont fourni des exemples de documents nécessaires à l'atteinte des pré-requis du programme Hôpital numérique :
    - Centre Hospitalier d'Hyères ;
    - Centre Hospitalier Régional et Universitaire de Tours ;
    - Centre Hospitalier Départemental Georges Daumézon de Fleury-les-Aubrais ;
    - Centre Hospitalier de Mâcon ;
    - Centre Hospitalier de Vienne ;
    - Centre Hospitalier de l'Agglomération de Nevers ;
    - Centre Hospitalier de Châteaubriant ;
    - Centre Hospitalier Intercommunal de Créteil (CHIC) ;
    - Centre Psychothérapique de l'Ain (CPA) ;
    - Centre Hospitalier de Saint-Amand-les-Eaux ;
    - Centre Hospitalier de Gonesse ;
    - Centre Hospitalier Intercommunal de la Lauter de Wissembourg ;
    - Institut Curie.

  Les modèles de documents-type contenus dans les fiches pratiques de l'outil ont été principalement établis sur la base de ces documents transmis par les établissements de santé.