MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

NOTE D'INFORMATION N° DGOS/PF/2023/94 du 15 juin 2023 visant à informer les établissements de santé de la publication d'un guide d'aide à la préparation au volet numérique du Plan blanc

Le ministre de la santé et de la prévention

à

Mesdames et Messieurs les directeurs généraux
des agences régionales de santé

Référence	NOR : SPRH2315112N (numéro interne : 2023/94)
Date de signature	15/06/2023
Emetteur	Ministère de la santé et de la prévention Direction générale de l'offre de soins
Objet	Informer les établissements de santé de la publication d'un guide d'aide à la préparation au volet numérique du plan blanc.
Contacts utiles	Sous-direction du pilotage de la performance des acteurs de l'offre de soins Mél. : bast.bidar@sante.gouv.fr Mél. : nicolas.voss@sante.gouv.fr
Nombre de pages et annexe	2 pages et 1 annexe (84 pages) Annexe : Plan blanc numérique – guide d'aide à la préparation pour les établissements
Résumé	La présente note a pour objet d'informer les établissements de santé de la publication d'un guide d'aide à la préparation au volet numérique du plan blanc. Ce guide fournit une aide méthodologique aux établissements de santé qui sont engagés dans la mise en œuvre d'un plan de réponse aux incidents numériques et notamment des cyberattaques.
Mention Outre-mer	Ces dispositions s'appliquent aux Outre-mer, à l'exception de la Polynésie française, de la Nouvelle-Calédonie et de Wallis et Futuna.
Mots-clés	Panne informatique – Cyberattaque – Cybersécurité – Incidents numériques.
Classement thématique	Etablissements de santé – Organisation
Texte de référence	Néant
Rediffusion locale	Directions des établissements de santé
Inscrite pour information à l'ordre du jour du CNP du 9 juin 2023 – N° 44	
Document opposable	Oui
Déposée sur le site Légifrance	Non
Publiée au BO	Oui
Date d'application	Immédiate

Les incidents numériques et notamment les cyberattaques se sont multipliés et touchent fréquemment les établissements de santé. Les signalements d'incidents de sécurité ont doublé en 2021 par rapport à 2019 et 2020 dans le secteur de la santé.

La sécurité des systèmes d'information et le traitement des incidents sont devenus une priorité pour les pouvoirs publics car ces attaques peuvent directement menacer non seulement la sécurité du système d'information de l'établissement, mais également la sécurité des patients qui sont pris en charge. Ces attaques peuvent neutraliser les communications internes et externes de l'établissement de santé et perturber l'offre de soins.

Ce guide est composé de trois parties :

- La première partie précise les mesures préventives de sécurité numérique à mettre en œuvre afin de prévenir, diminuer l'exposition et maîtriser le risque numérique ;
- La deuxième partie du guide décrit les travaux de préparation à anticiper pour faire face à un incident numérique ;
- La troisième partie décrit l'organisation des soins en mode dégradé.

D'un point de vue pratique, cinq fiches réflexes sont proposées pour identifier les actions à mettre en œuvre par anticipation pour se préparer au risque numérique.

Vous trouvez en annexe de la présente note d'information, le guide d'aide à la préparation du volet numérique du plan blanc.

Vous voudrez bien assurer la diffusion de cette note d'information accompagnée du guide d'aide à la préparation du volet numérique du plan blanc aux directeurs des établissements de santé.

Pour le ministre et par délégation :
La directrice générale de l'offre de soins,

Marie DAUDÉ

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

Direction générale
de l'offre de soins

PLAN BLANC NUMÉRIQUE

ÉTABLISSEMENTS DE SANTÉ

GUIDE D'AIDE À LA PRÉPARATION

Sommaire

SYNTHESE 1

AVANT-PROPOS 3

INTRODUCTION 4

PARTIE 1 : PREVENIR LE RISQUE NUMERIQUE 6

CHAPITRE 1 : MAITRISER SES SYSTEMES D'INFORMATION 6

1. **Disposer de ressources humaines pour sécuriser le système d'information 6**
   - 1.1 Désignation d'un responsable de la sécurité des systèmes d'information 6
   - 1.2 Des ressources techniques adaptées au maintien en sécurité 6
   - 1.3 L'implication du service en charge des systèmes d'information 7
   - 1.4 La sensibilisation du personnel 7
2. **L'importance des cartographies du système d'information 7**
   - 2.1 La nécessité de réaliser une cartographie précise 7
   - 2.2 Le contenu de la cartographie 8
3. **L'analyse de risque 9**
   - 3.1 Les typologies de menace 9
   - 3.2 L'importance d'identifier les applications métiers critiques 9
   - 3.3 Le repérage des applications métiers hors du schéma directeur 10
   - 3.4 L'identification des vulnérabilités 10
   - 3.5 Des structures de soins qui partagent des données sensibles 11
   - 3.6 La prise en compte des liaisons externes 11
   - 3.7 Une attention particulière aux opérateurs de télémaintenance 11
   - 3.8 Les risques liés aux dispositifs médicaux connectés 12
   - 3.9 La gestion des centrales de surveillance 12
   - 3.10 Les outils de collaboration cliniques inter-établissements 12
   - 3.11 Evaluer la vulnérabilité de l'annuaire central 13

CHAPITRE 2 : FORMALISER UN PLAN DE MISE EN CONFORMITE ADAPTE 15

1. **Formaliser des actions pour sécuriser le système d'information 15**
   - 1.1 Les directives NIS : sécurité des réseaux et des systèmes d'information 15
   - 1.2 La politique de sécurité des systèmes d'information (PSSI) 15
   - 1.3 Le plan d'action de sécurité des systèmes d'informations 16
   - 1.4 Les 23 règles de sécurité des 135 établissements supports de GHT 16
   - 1.5 Définir les systèmes d'information essentiels 16
2. **Des mesures prioritaires à mettre en œuvre 17**
   - 2.1 Le référentiel des 43 mesures prioritaires de sécurité des systèmes 17
   - 2.2 La gestion des correctifs de sécurité, une mesure prioritaire majeure 17

2.3 Cloisonner l'architecture, une mesure prioritaire majeure 17
2.4 Maîtriser l'authentification des accès et des mots de passe 18
2.5 Protéger la messagerie professionnelle 18
2.6 Des campagnes aléatoires de « *phishing* » 18
2.7 Identifier les données sensibles et les flux stratégiques 19
2.8 Le référentiel Identifiant National de Santé : INS 19
2.9 La nécessité de mettre en œuvre des audits réguliers 19

PARTIE 2 : ELABORER LE VOLET NUMERIQUE 21

CHAPITRE 1 : LES MODALITES DE MISES EN ŒUVRE 21

1. L'articulation avec les plans ORSAN, Gestion des tensions, PCA, PRA 21

1.1 Le plan ORSAN : un plan de réponse régional 21
1.2 Le plan de gestion des tensions hospitalières 21
1.3 L'articulation avec les plans de continuité/reprise d'activité 22
1.4 Le plan de continuité d'activité du système d'information : PCA 23
1.5 Le plan de reprise d'activité du système d'information : PRA 23

2. Le volet numérique 24

2.1 L'intérêt de disposer d'un volet numérique 24
2.2 Un volet numérique qui pourra être mutualisé au sein du GHT 24
2.3 Les critères de déclenchement du volet numérique 25
2.4 La confidentialité du volet numérique 25

3. Coordonner et impliquer l'ensemble des acteurs 25

3.1 L'implication des acteurs pour l'élaboration du plan 25
3.2 La coordination par l'ARS en lien avec le GRADeS 26
3.3 Un appui des agences nationales : ANS, ANSSI 26

4. Une cellule de crise : décision et opération 27

4.1 Un organe de pilotage de la crise numérique 27
4.2 La désignation d'un directeur médical de crise DMC 28
4.3 Le rôle de la cellule de crise hospitalière 28
4.4 La cellule de crise hospitalière communique régulièrement en interne 29
4.5 La logistique nécessaire à une cellule de crise 29
4.6 Un vecteur de communication rapide et sécurisé 29

5. La mobilisation de ressources techniques expertes 30

5.1 Des ressources techniques d'intervention 30
5.2 Une équipe « réponse à incident » mutualisée au sein du GHT 30
5.3 L'appui de l'ANS et de l'ANSSI 31

6. Les étapes à suivre lors d'un incident numérique 31

6.1 Des mesures de gestion adaptées à la nature de l'incident numérique 31

7. La conservation des preuves, le dépôt de plainte et la demande de rançon 32

7.1 La collecte des preuves des systèmes attaqués 32
7.2 Le dépôt de plainte 33
7.3 La gestion de la demande de rançon 33

CHAPITRE 2 : LES ELEMENTS GENERAUX A PREPARER 35

1. **Les éléments de préparation généraux 35**

1.1 Des travaux d'anticipation 35
1.2 Une réponse adaptée aux principaux scenarii 35
1.3 Une stratégie de réponse commune au sein du GHT ou de la région 36
1.4 Une description de l'offre de soins et des prises en charge à risque 36
1.5 Un stock stratégique idéalement mutualisé 36
1.6 L'obligation de réaliser des exercices 37
1.7 Des tests d'intrusion pour évaluer la sécurité globale 37

2. **Les travaux préparatoires à la communication 38**

2.1 Des outils de communication à préparer 38
2.2 La communication interne 38
2.3 La communication externe 38
2.4 Un dispositif d'information auprès des patients et des familles 39
2.5 Les moyens alternatifs de communication 39

3. **Le signalement interne d'une anomalie 40**

3.1 Le signalement interne d'une anomalie du système d'information 40
3.2 Définir des critères d'alertes internes 40

4. **La procédure de signalement des incidents numériques 40**

4.1 Informer le personnel pour sécuriser le système d'information 40
4.2 Le cadre réglementaire du signalement d'un incident numérique 41
4.3 Le signalement aux autorités compétentes 42
4.4 Les éléments à recueillir lors du signalement 42

5. **Une veille sur les *scenarii* et vecteurs d'attaque fréquents 43**

5.1 Une veille permanente sur les typologies d'attaque 43
5.2 Les vecteurs d'attaque fréquents 43
5.3 L'acte de malveillance 44

CHAPITRE 3 : SE PREPARER AUX ETAPES A SUIVRE 45

1. **La détection et l'identification du périmètre de la cyberattaque 45**

1.1 Détecter et reconnaître une perturbation informatique 45
1.2 La mise en place d'outils de détection efficaces 45
1.3 Vérifier la capacité de détecter les codes malveillants polymorphes 46
1.4 Evaluer la pertinence de mettre en œuvre la technologie EDR 46
1.5 Identifier le périmètre et le chemin de compromission suivi 47
1.6 Collecter les journaux d'incident des éléments de sécurité 47

2. **Le recensement des systèmes corrompus et la qualification de l'incident 47**

2.1 Identifier les systèmes corrompus 47
2.2 Contrôler l'intégrité des sauvegardes 48
2.3 La qualification va déterminer le déclenchement du volet numérique 48

3. **Le confinement des zones affectées pour réduire la surface d'attaque 49**

3.1 Le confinement des systèmes corrompus pour endiguer l'attaque 49
3.2 Des stratégies de confinement différentes selon le type d'incident 49
3.3 Des mesures immédiates pour réduire la surface d'attaque 49

4. **Le fonctionnement du système d'information en mode dégradé 50**

4.1 Des mesures temporaires à mettre en œuvre 50
4.2 Des infrastructures temporaires 50
4.3 Une vigilance à la saturation du réseau 51

5. **L'éradication par la correction des vulnérabilités 51**

5.1 La suppression des codes malveillants 51
5.2 La correction des vulnérabilités 51

6. **La stratégie de sauvegarde pour anticiper l'étape de restauration 52**

6.1 Des sauvegardes déconnectées du système d'information 52
6.2 Une attention particulière pour les données et applications critiques 53

7. **La restauration des systèmes d'information corrompus 53**

7.1 L'application du plan de reprise d'activité PRA 53
7.2 Restaurer les systèmes et données endommagés 53
7.3 Des tests de restauration éprouvés et testés 54
7.4 La restauration des applications, un processus qui peut être long 54

8. **La reconstruction des systèmes compromis 54**

8.1 La phase de reconstruction 54
8.2 Le choix de reconstruire les applicatifs au sein d'une zone sécurisée 54

9. **Arbitrer la sortie de crise 55**

9.1 Définir des critères de sortie de crise 55
9.2 Arbitrer la suppression du fonctionnement dégradé 55

10. **Effectuer un retour d'expérience post attaque rapide 55**

10.1 Analyser les forces et les faiblesses 55
10.2 Tirer les enseignements 55
10.3 Une communication à adapter lors des retours d'expérience 56

PARTIE 3 : L'ORGANISATION DES SOINS 58

CHAPITRE 1 : L'IMPACT SUR L'ORGANISATION DES SOINS 58

1. **Le pilotage de la continuité des soins 58**

1.1 Le pilotage de l'ARS 58
1.2 Organiser la continuité des soins avec les établissements du territoire 58
1.3 Vérifier la capacité d'admission de nouveaux patients 58
1.4 Choisir de transférer certains patients vers d'autres établissements 59
1.5 Quantifier en continu l'impact sur la qualité et la sécurité des soins 59

2. **L'organisation des soins en mode dégradé 59**

2.1 Le réseau téléphonique et la messagerie 59
2.2 La gestion du poste de travail : déconnecter et éteindre son ordinateur 60
2.3 L'offre de soins 60
2.4 Les dispositifs médicaux 61
2.5 Les fonctions logistiques 61
2.6 La gestion centralisée/technique des bâtiments (GTC/GTB) 61
2.7 La gestion administrative 62

3. **Les procédures du mode dégradé et les exercices 62**

3.1 Des procédures documentées stockées hors du système d'information 62
3.2 Des procédures connues et testées grâce à des exercices réguliers 62
3.3 Des exercices réguliers nécessaires 63
3.4 Une agilité des services de soins 63

4. **Le soutien nécessaire aux équipes 63**

4.1 Veiller au soutien des équipes 63

CHAPITRE 2 : LA PRISE EN CHARGE EN MODE DEGRADE 64

1. **L'identification des activités critiques 64**

1.1 Des modalités d'organisation en fonction des composants affectés 64
1.2 L'identification des services de soins critiques 64

2. **La prise en charge des patients en mode dégradé 64**

2.1 Le dossier patient informatisé 64
2.2 Le PC de sauvegarde 65
2.3 Le SAS et le SAMU-Centre 15 65
2.4 Sécurisation des communications des SAS et SAMU-Centre 15 66
2.5 L'accueil aux urgences 66
2.6 Le bloc opératoire 67
2.7 La stérilisation des dispositifs médicaux 68
2.8 Les soins critiques : réanimation, soins intensifs, soins continus 69
2.9 L'imagerie médicale 70
2.10 Le laboratoire de biologie médicale 72
2.11 La pharmacie à usage intérieur PUI 73
2.12 L'actualisation des données recueillies lors du mode dégradé 74

RÉDACTION ET REMERCIEMENTS 76

SYNTHESE

Les incidents numériques et notamment les cyberattaques se sont multipliés et touchent les établissements de santé. Dans le secteur de la santé, les signalements de ces incidents ont doublé en 2021 par rapport à 2019 et 2020. La sécurité des systèmes d'information et le traitement des incidents sont devenus une priorité pour les pouvoirs publics dans la mesure où ces attaques peuvent directement menacer non seulement la sécurité du système d'information de l'établissement, mais également la sécurité des patients pris en charge.

Il est donc nécessaire d'élaborer un volet numérique dans le plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles qui décrit les mesures activables en fonction de la nature, de l'ampleur et de la cinétique de l'incident numérique (panne, cyberattaque…). Ce volet numérique vise également à identifier les mesures à mettre en œuvre en amont pour adopter des stratégies de défense en adéquation avec le paysage actuel des menaces.

Ce guide d'aide à la préparation du risque numérique vise à fournir un cadre méthodologique et pratique pour prévenir le risque numérique et adopter une conduite collective visant à gérer et sortir au mieux d'une crise numérique en se reposant sur la réglementation et en faisant référence aux outils techniques existants.

Ce guide d'aide à la préparation du risque numérique est composé de trois parties.

La première partie précise les mesures préventives de sécurité numérique à mettre en œuvre afin de prévenir, diminuer l'exposition et maîtriser le risque numérique. Il s'agit notamment de désigner un responsable de la sécurité des systèmes d'information, d'assurer la sensibilisation du personnel au risque numérique, d'effectuer une cartographie précise et de réaliser une analyse des risques de l'ensemble du système d'information. Une attention particulière sera portée aux risques de vulnérabilité du système d'information et notamment de la messagerie professionnelle qui est un vecteur important d'infection du poste de travail utilisé par les assaillants pour s'introduire dans le système d'information de l'établissement de santé. Au regard de cette analyse des risques, un plan de mise en sécurité devra être mis en place.

La deuxième partie vise à décrire les travaux de préparation à effectuer pour disposer d'une réponse adaptée à l'incident numérique. Le volet numérique décrit les moyens opérationnels adaptés aux *scenarii* de crise. Il est rappelé l'articulation du volet numérique avec les différents plans existants et notamment son lien avec le dispositif régional ORSAN. Le volet numérique devra intégrer l'ensemble des plans déjà existants et notamment les plans de continuité/reprise d'activité du système d'information.

Bien entendu, l'élaboration de ce volet numérique devra mobiliser l'ensemble des acteurs de l'établissement.

En lien avec les services de l'agence régionale de santé (ARS) et le Groupement Régional d'Appui au Développement de la e-Santé (GRADeS), il est proposé de mutualiser, au niveau du groupement hospitalier de territoire (GHT), la démarche de réponse à un incident numérique et notamment d'évaluer la nécessité de disposer d'une équipe experte « réponse à incident » au sein du GHT ou au sein de la région, qui pourra intervenir en cas de besoin.

Un point d'attention particulier est à porter sur les travaux préparatoires à la communication compte tenu de l'importance des médias et des réseaux sociaux notamment.

La chaîne d'alerte lors d'un incident numérique est également précisée ainsi que les modalités d'appui des agences nationales (ANS, ANSSI).

Enfin, la troisième partie précise l'organisation des soins à mettre en œuvre en cas d'incident numérique et notamment le fonctionnement des services de soins en mode dégradé. Il est notamment indiqué de qualifier en continu l'impact du mode dégradé sur la qualité et la sécurité des soins afin de vérifier que les soins prodigués sont en adéquation avec la charge en soins requise par les patients.

Des exemples d'organisation en mode dégradé sont proposés pour quelques activités : SAS, SAMU-Centre 15, urgence, pharmacie à usage intérieur, laboratoire, imagerie, bloc opératoire, stérilisation, soins critiques.

Lors d'une cyberattaque, la stratégie de mise en œuvre d'un fonctionnement en mode dégradé impose d'évaluer l'impact sur la qualité des soins et la vérification en continu que les soins prodigués dans des conditions dégradées sont toujours appropriés à la nature des patients pris en charge. De la même façon, au regard de la capacité des services de soins à assurer des prises en charge en mode dégradé, il sera nécessaire de quantifier la capacité de l'établissement à accueillir de nouveaux patients. Cette évaluation permettra également de disposer en continu, d'éléments de décision pour le transfert inter-hospitalier éventuel de patients vers un établissement tiers, en collaboration avec l'ARS.

D'un point de vue pratique, cinq fiches réflexes sont proposées pour identifier de façon claire les actions à mettre en œuvre par anticipation pour préparer la crise numérique.

Le retour d'expérience après un incident numérique et notamment une cyberattaque fait partie intégrante du processus, car il permet aux établissements de santé de réduire le risque de futures attaques et de mieux se protéger et ainsi protéger les patients pris en charge. L'appui de personnes extérieures à la structure, neutres, est à envisager. Une attention particulière sera portée sur le contenu des informations diffusées au grand public et notamment l'identification des moyens de défense et de sécurisation des composants critiques d'un établissement de santé.

En cas de cyberattaque, il est rappelé que le paiement d'une rançon est exclu, car il entretient le système frauduleux et ne garantit pas la récupération des données ou des systèmes compromis. Il n'est pas recommandé de négocier avec l'assaillant. Seules des personnes expertes en la matière (forces de l'ordre, négociateur spécialisé…) peuvent le faire si elles le jugent utile.

Le volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles peut être considéré comme confidentiel et même stratégique pour les établissements de santé désignés opérateurs de services essentiels (OSE), car il dévoile la stratégie de réponse face à un incident numérique et notamment une cyberattaque. Certaines informations et modalités de mise en œuvre du volet numérique doivent être protégées, notamment pour ne pas permettre leur exploitation par des personnes malveillantes.

AVANT-PROPOS

Les acteurs du système de santé doivent pouvoir se préparer au traitement d'un incident numérique, notamment une cyberattaque, et se mobiliser en s'appuyant sur des ressources internes et externes.

Face à cet enjeu majeur, tout établissement de santé doit renforcer sa préparation au risque numérique et doit pour cela élaborer un volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles. Ce volet numérique décrira les mesures graduées activables en fonction de la nature, de l'ampleur et de la cinétique de l'incident numérique (panne, cyberattaque…).

Les conséquences sur l'offre de soins doivent être également anticipées et faire l'objet d'une organisation pour assurer la continuité des soins qui est *de facto* prise en compte dans le plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles de l'établissement.

Ce guide d'aide à la préparation du volet numérique a vocation à faciliter l'élaboration des travaux de préparation au risque numérique au sein des établissements de santé.

Ce cadre de préparation et de réponse s'intègre naturellement au plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles avec pour objectif d'assurer la gestion de l'incident numérique et la restauration dans les meilleurs délais du ou des systèmes d'information compromis.

Les actions préventives au risque numérique nécessitent d'être mutualisées au sein du GHT pour garantir une stratégie de sécurité des systèmes d'information commune.

La réponse au risque numérique sur l'offre de soins doit s'envisager à l'échelon du GHT et plus largement d'un territoire de santé avec tous les acteurs concernés dans une démarche de construction commune et coordonnée de la réponse.

À ce titre, l'agence régionale de santé (ARS) coordonne la gestion des conséquences de l'incident entre les opérateurs de soins par la mise en œuvre de la disposition spécifique transversale « cyber » du dispositif ORSAN.

Enfin, ce guide a été plus spécifiquement réalisé pour les établissements sanitaires et n'est ainsi pas totalement adapté au secteur médico-social. Les acteurs du médico-social travaillent actuellement sur un plan bleu numérique destiné aux établissements et services médico-sociaux (ESMS). Une des pistes pourrait être de retravailler les éléments de ce guide pour aboutir à une version destinée aux ESMS. En attendant et en complément, l'ANS a publié « 13 questions pour être incollable en matière de cyber sécurité » à destination des ESMS.

INTRODUCTION

Les incidents numériques et notamment les cyberattaques, aux conséquences parfois majeures, se sont multipliés et touchent particulièrement les établissements de santé. Les signalements d'incidents de sécurité ont doublé en 2021 par rapport à 2019 et 2020 dans le secteur de la santé. En 2022, ces signalements restent encore à un niveau de déclaration très élevé.

Pour répondre à ces cyberattaques croissantes, le ministre de l'Intérieur, Gérald Darmanin, celui de la Santé et de la Prévention, François Braun, et le ministre délégué au Numérique, Jean-Noël Barrot, ont annoncé la création d'un « plan blanc numérique » pour doter les établissements de santé des réflexes et pratiques à adopter si un incident numérique survient.

En outre, le besoin croissant de coordination entre les établissements de santé nécessite d'ouvrir davantage les systèmes d'information pour permettre l'échange et le partage de données de santé entre les professionnels impliqués dans la prise en charge des patients, qu'ils soient du même établissement, du même GHT ou extérieurs.

Bien que les établissements de santé se soient engagés depuis plusieurs années dans la sécurisation de leurs systèmes d'information grâce à des moyens importants délégués par les pouvoirs publics, des efforts significatifs doivent encore être réalisés.

Il est donc nécessaire pour chaque établissement de santé de construire un « volet numérique » robuste au sein de son plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles pour apporter une réponse efficace, et en temps réel, à un incident numérique de type cyberattaque notamment.

Bien entendu, la mise en œuvre des mesures de sécurisation pour prévenir le risque numérique est un prérequis indispensable avant l'élaboration d'un plan blanc numérique.

Le volet numérique permettra de mobiliser immédiatement les moyens techniques et humains disponibles pour faire face à un incident numérique et notamment une cyberattaque.

Ce volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles devra s'appuyer notamment sur :

- Le « plan de continuité d'activité du système d'information - PCA » qui vise à maintenir l'activité de l'établissement lors d'un incident numérique et notamment, de décrire l'infrastructure de secours pour permettre la reprise automatique et immédiate du système d'information ;
- Le « plan de reprise d'activité du système d'information - PRA » qui décrit l'ensemble des procédures détaillées pour restaurer chacun des composants majeurs et applications métiers corrompus.

L'organisation à prévoir nécessite de prendre en compte le temps important nécessaire pour restaurer l'ensemble des composants du système d'information affectés.

Ce guide n'a toutefois pas vocation à apporter une réponse exhaustive à toutes les typologies d'incident numérique.

Compte tenu des disparités des organisations, il appartient aux directeurs des établissements de santé en collaboration avec les responsables des services des systèmes d'information, le responsable de la sécurité des systèmes d'information (RSSI), de décliner ces orientations en fonction de leurs organisations locales et de les adapter le cas échéant.

Les lignes directrices proposées restent des orientations générales qui seront actualisées au fur et à mesure de l'évolution des connaissances et des menaces. Ce guide n'impose aucune disposition réglementaire nouvelle.

Ce guide est mis en ligne sur le site du ministère de la Santé et de la Prévention.

PARTIE 1 : PREVENIR LE RISQUE NUMERIQUE

CHAPITRE 1 : MAITRISER SES SYSTEMES D'INFORMATION

1. Disposer de ressources humaines pour sécuriser le système d'information

1.1 Désignation d'un responsable de la sécurité des systèmes d'information

Le directeur général de l'établissement de santé, également directeur de la cellule de crise hospitalière, doit désigner un responsable de la sécurité des systèmes d'information (RSSI) pour mettre en place des mesures visant à limiter le risque de survenue d'un incident numérique et de cyberattaque en particulier : il s'agit du prérequis P3.1 du programme Hôpital numérique et la mesure prioritaire 6 issue de la dimension Sécurité du référentiel MATURIN'H.

Le RSSI sera chargé de promouvoir et accompagner les bons usages et les pratiques de sécurisation au quotidien au sein des services de soins. Cette fonction pourra être idéalement mutualisée à l'échelle du GHT, voire externalisée.

Interlocuteur clé, il a pour mission de sensibiliser l'ensemble des acteurs de l'établissement de santé à la prévention des risques numériques et notamment des cyberattaques, de définir des actions de sécurisation et d'en contrôler l'application. Pour cela, il organise, en mode collaboratif, des diagnostics, des analyses de postes, des audits de sécurité. Il est l'interlocuteur privilégié du personnel et de la direction de l'établissement sur la sécurité des systèmes d'information et notamment de la cybersécurité.

Son rôle est d'inciter les professionnels de soins et l'ensemble des personnels à tenir compte des mesures de prévention pour limiter les risques d'intrusion. Pour cela, le RSSI mène régulièrement des actions de sensibilisation et d'information, des simulations, et organise des formations à destination des personnels. Il facilite la remontée des informations concernant la réalité du terrain.

Le RSSI rend compte a minima semestriellement à la gouvernance de l'établissement de l'évolution des risques numériques et des avancées dans la mise en conformité du système d'information (prérequis du programme Ségur numérique usage en établissements de santé - SUN-ES).

1.2 Des ressources techniques adaptées au maintien en sécurité

Les systèmes d'information constituent un levier pour l'amélioration de la qualité et de l'organisation des soins. Il est nécessaire d'adapter l'effectif des ressources techniques dédiées à la sécurisation du système d'information, au regard des tâches à accomplir. Un point d'attention sera porté au niveau de formation, d'expérience et de compétence du personnel.

1.3 L'implication du service en charge des systèmes d'information

L'intégration de la cybersécurité dans le cycle de vie des processus et applicatifs acquis au sein des établissements de santé est une étape clé pour parvenir aux exigences attendues. Une attention particulière devra être portée par la direction des systèmes d'information à ce risque lors des phases de conception et de déploiement des applicatifs.

Il est donc fondamental d'intégrer systématiquement la cybersécurité lors des différentes étapes de la procédure de passation de marchés et notamment au sein des dispositions relatives au processus de télémaintenance.

Des échanges réguliers entre les services biomédicaux et la direction des systèmes d'information sont nécessaires pour anticiper les organisations à mettre en œuvre dans le cadre de la surveillance centralisée des dispositifs médicaux notamment.

1.4 La sensibilisation du personnel

Les personnels des établissements de santé doivent être informés des menaces qui visent le parc numérique et les systèmes d'information hospitaliers. Il est nécessaire d'inscrire une action de sensibilisation à la sécurité des systèmes d'information dans le plan de formation annuel des personnels de la structure et par la réalisation d'exercices cadres ou en conditions réelles.

Lors des sessions d'accueil des nouveaux personnels, une sensibilisation forte devra être systématiquement proposée. Il s'agira par un document de validation, de s'assurer que l'ensemble des mesures de sécurité préconisées par l'établissement soient bien comprises par les nouveaux arrivants.

Un affichage permanent des principales recommandations dans les services permettra de garantir une application des règles d'hygiène en matière de sécurité numérique. Un document devra formaliser la prise en compte des éléments de sécurité.

2. L'importance des cartographies du système d'information

2.1 La nécessité de réaliser une cartographie précise

Les équipes qui exploitent et maintiennent en condition opérationnelle le système d'information des établissements de santé doivent pouvoir s'appuyer sur une documentation fiable et à jour. Il est donc nécessaire de réaliser une cartographie complète des ressources informatiques de l'établissement ainsi que ses connexions internes et externes.

Cette cartographie est par ailleurs un outil indispensable au pilotage de l'évolution du système d'information en particulier dans les contextes de mutualisation au sein du GHT.

Elle constituera également le document « socle » lors d'un incident numérique pour faciliter la prise de décision et contribuera au ciblage des mesures de protection, de défense et de résilience du système d'information.

Elle permettra notamment de définir l'ordre de remise en service des applications métiers corrompues en cas d'attaque.

Il est indispensable de prendre conscience que les informations contenues dans cette cartographie peuvent s'apparenter à des données sensibles, voire confidentielles. Il est donc recommandé d'en limiter l'accès, notamment en ce qui concerne les informations des systèmes de sécurité mis en œuvre.

L'ANSSI fournit des recommandations en ce sens.

2.2 Le contenu de la cartographie

Cette cartographie précisera les éléments fonctionnels prioritaires qui pourraient, en cas de défaillance, impacter fortement la prise en charge des patients au sein de l'établissement. Cette cartographie des éléments fonctionnels prioritaires permettra de faciliter la création d'infrastructures temporaires si nécessaire.

L'ensemble des actifs matériels, logiciels métiers et de service ainsi que l'ensemble des connexions réseaux seront décrits et identifiés à travers des listes détaillées et schémas, dont les contenus sont alignés et régulièrement actualisés. Logiciels et équipements seront correctement répertoriés pour faciliter les travaux ultérieurs tels que l'application de correctifs.

Une liste comportera, par exemple, les commutateurs, les routeurs, les passerelles protocolaires, les interfaces et les interconnexions avec l'extérieur (internet, réseaux privés, partenaires, etc.). Pour chaque équipement, la cartographie devra préciser notamment les emplacements physiques (bâtiment, pièce, armoire, baie). La cartographie devra également permettre de localiser les serveurs stockant des informations sensibles de l'entité.

Une cartographie des prestataires (numériques et autres) ayant potentiellement un impact sur la continuité de fonctionnement de l'établissement devra également être réalisée.

Les liaisons avec les partenaires externes seront également décrites : internet, réseaux privés, partenaires. Il s'agira notamment d'identifier les liens de la « chaîne d'approvisionnement numérique ».

L'établissement pourra se baser sur les éléments précisés dans la règle 6 « cartographie » de l'arrêté du 14 septembre 2018 relatif à la sécurité des réseaux et systèmes qui s'applique aux 135 établissements supports de GHT.

Une représentation plus macroscopique pourra aussi être utilisée pour obtenir un niveau de granularité plus général et favoriser la pérennité de la cartographie.

L'exhaustivité des liens au sein du système d'information sera essentielle pour fiabiliser la lecture des impacts de sécurité numérique.

L'utilisation d'un logiciel spécifique de modélisation du système d'information peut s'avérer utile pour permettre de formaliser dans le détail l'ensemble des données et connexions internes/externes.

Enfin, la mise à jour régulière de la cartographie est une étape indispensable de la démarche, notamment lors d'une opération de réhabilitation/restructuration.

Le DSI et le RSSI veillent à actualiser la cartographie applicative dans la plate-forme nationale déclarative oSIS (Observatoire des Systèmes d'Information de Santé).

Pour aller plus loin, le guide « Cartographie du système d'information, guide d'élaboration en cinq étapes » publié par l'ANSSI présente une démarche adaptée aux besoins opérationnels des organisations et propose une approche pratique et progressive pour avancer pas à pas dans l'élaboration d'une cartographie.

3. L'analyse de risque

3.1 Les typologies de menace

Avant l'élaboration d'un plan de mise en conformité du système d'information (homologation), une analyse approfondie des risques est essentielle afin que des mesures de sécurisation puissent être prises. Cette analyse des risques nécessite d'être prioritairement basée sur la fonctionnalité opérationnelle de l'établissement, c'est-à-dire le maintien des prises en charge des patients.

Dans un premier temps, il est nécessaire d'identifier les menaces auxquelles les établissements de santé peuvent être confrontés. Il est possible de classer les menaces selon la typologie suivante :

- Action malveillante (cyberattaque, action d'origine interne…) ;
- Sinistre (inondation, incendie, dégât des eaux, perte de climatisation, séisme…) ;
- Perte de services essentiels ;
- Compromission des données ;
- Défaillance technique.

Plusieurs méthodologies d'analyses des risques peuvent être mises en œuvre. La méthodologie *EBIOS Risk Manager* approuvée par l'ANSSI peut permettre de réaliser une analyse des risques complète d'un système d'information avant son déploiement.

3.2 L'importance d'identifier les applications métiers critiques

Pour l'ensemble des systèmes d'information nécessaires au fonctionnement de l'établissement de santé, il sera nécessaire d'évaluer la criticité sur une échelle de [1 à 4] [1] de l'interruption en fonction de la durée d'indisponibilité.

[1] Méthode Ebios Manager : https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

Pour permettre d'évaluer de façon rapide la gravité d'un incident numérique, il est nécessaire de connaître l'impact de cet incident sur les applications métiers critiques de l'établissement. Il s'agit des systèmes d'information dont l'interruption plus ou moins prolongée aurait un impact significatif sur le fonctionnement de l'établissement et notamment sur la prise en charge des patients.

Plusieurs tranches horaires d'indisponibilité pourront être proposées (0-4heures ; 4-8heures…). La durée d'interruption maximale admissible peut être estimée en minutes pour les applications les plus indispensables.

Les récents retours d'expérience traduisent des durées d'indisponibilité de logiciels métiers importantes.

De la même façon, pour prioriser la remise en fonctionnement de l'établissement en cas de crise, il est nécessaire en amont d'identifier les systèmes d'information clés qui permettent d'assurer la continuité des prises en charge.

Un facteur de criticité et une durée maximale admissible d'indisponibilité (évaluée sous l'angle médical et technique) devra être associé à chaque composant du système d'information.

3.3 Le repérage des applications métiers hors du schéma directeur

Dans le cadre des travaux relatifs à la cartographie, il sera nécessaire de repérer les applications métiers utilisées qui ne sont pas répertoriées au sein de l'inventaire de la direction du système d'information de l'établissement. Il peut s'agir d'applications de partage de données utilisées dans le cadre d'une étude clinique par exemple ou d'applications métiers qui permettent la mutualisation d'informations avec des entités extérieures.

En effet, ces applications pourraient ne pas être totalement conformes à la politique générale de sécurité des systèmes d'information (PGSSI).

Il est nécessaire d'en faire un inventaire précis et d'en proposer un cadre sécurisé.

3.4 L'identification des vulnérabilités

Pour chaque type de menace, il est nécessaire d'identifier les actifs potentiellement impactés et d'en préciser les points de fragilité, autrement dit les vulnérabilités (absence de dispositif d'alimentation secours, absence de système de sauvegarde, obsolescence d'un système d'exploitation, absence de clauses d'exclusion d'accès, etc). Cette étape est le point essentiel d'amorçage de la démarche de sécurisation du système d'information de l'établissement.

Ces vulnérabilités étant précisées, il s'agit d'évaluer la probabilité de « réalisation du risque » par rapport à une menace donnée.

Il s'agit ensuite d'évaluer l'impact de l'occurrence du risque sur les différentes composantes d'un établissement :

- Production des soins : la prise en charge des patients est impactée ;
- Administratif : l'identité patient, le codage, la facturation, l'encaissement sont impactés ;
- Logistique : la gestion des déchets, le transport, la restauration des patients sont impactés ;
- Volet légal et réglementaire : le respect d'obligation légale ou réglementaires est impacté ;
- Recherche : la poursuite de travaux de recherche est impactée ;
- Image : la réputation de l'établissement est impactée.

Les risques étant ainsi caractérisés, des niveaux de gravité peuvent leur être associés, combinant leur impact et la probabilité de survenue.

3.5 Des structures de soins qui partagent des données sensibles

Les structures de soins d'un territoire de santé sont souvent très étroitement liées les unes aux autres, partageant des informations confidentielles sur les patients à prendre en charge et établissant régulièrement des échanges de données avec les agences nationales pour la tarification à l'activité par exemple.

La mise en œuvre de contre-mesures immédiates nécessite d'être prévue.

Si les différentes phases d'un incident numérique ne sont pas toujours prévisibles, il est indispensable de travailler sur des protocoles et des conduites à tenir.

3.6 La prise en compte des liaisons externes

Une gestion de droits spécifiques pour les fournisseurs, avec un classement par niveau d'autorisation, permet de mieux piloter par priorité la criticité des applications tierces.

L'analyse des risques doit prendre en compte l'ensemble des éléments de la boucle interne du système d'information de l'établissement mais aussi d'une défaillance d'un réseau externe à l'établissement. Les récentes cyberattaques ont démontré que l'intrusion pouvait être réalisée en raison d'une défaillance liée à l'accès d'une entité extérieure au réseau de l'établissement.

Pour aller plus loin, l'ANS propose une fiche réflexe « Sécurisation de l'accès à distance des prestataires ».

3.7 Une attention particulière aux opérateurs de télémaintenance

Une attention particulière doit être portée sur les composants du système d'information de l'établissement qui nécessitent une accessibilité via un réseau public.

De la même façon, les opérateurs de télémaintenance doivent s'authentifier selon des conventions et protocoles techniques relevant de la politique générale de sécurité des systèmes d'information de l'établissement.

Pour aller plus loin, l'ANSSI propose une Note technique « Recommandations de sécurité relatives à la téléassistance ».

3.8 Les risques liés aux dispositifs médicaux connectés

Les établissements de santé améliorent la prise en charge des patients grâce à des systèmes d'information de plus en plus connectés et collaboratifs qui dépassent le périmètre géographique de l'établissement.

En effet, pour améliorer la prise en charge et favoriser la supervision des patients au sein des unités de soins, de nombreux dispositifs médicaux sont connectés au réseau (pousse seringue, pompe à perfusion, IRM…).

Des modalités de prise en charge des patients au sein des unités de soins intensifs de cardiologie par exemple, permettent de surveiller et localiser à distance les patients (télémétrie…).

Ces modalités de système et dispositifs connectés permettent notamment d'assurer une surveillance à distance des patients ou des échanges de données de patients.

3.9 La gestion des centrales de surveillance

Un travail préparatoire en lien avec les fabricants nécessite d'être mené pour déterminer la réponse à apporter en cas de défaillance du réseau de la centrale de surveillance liée aux dispositifs médicaux.

Une centrale de surveillance permet à l'équipe médicale et paramédicale de surveiller à distance et en temps réel tous les monitorings en cours par exemple.

En effet, en cas de coupure du réseau ou d'incident numérique, il est nécessaire de disposer d'une continuité de surveillance centralisée des patients notamment au sein des services de soins critiques (réanimation, soins intensifs, soins continus).

Une attention particulière sera portée pour les services de néonatologie et de réanimation néonatale.

3.10 Les outils de collaboration cliniques inter-établissements

De la même façon, les outils de collaboration cliniques (exemple : réunion de concertation pluridisciplinaire - RCP) doivent faire également l'objet d'une attention particulière au regard du risque numérique. Ils doivent être listés.

Des contre-mesures nécessitent d'être mises en œuvre en cas d'intrusion.

Une évaluation de la sécurité numérique de ces différents outils pourrait être sollicitée dans le cadre de leur acquisition.

3.11 Evaluer la vulnérabilité de l'annuaire central

L'annuaire central est la clé de voûte du système d'information d'un établissement.

Il centralise la gestion des comptes et des privilèges de l'ensemble des ressources informatiques de l'établissement. Cet annuaire permet aux administrateurs de gérer les droits d'accès de chaque utilisateur, de les authentifier lorsqu'ils se connectent et de déterminer les ressources auxquelles ils peuvent accéder.

Il stocke des informations sur les utilisateurs du réseau (mots de passe, etc.) et les ressources (serveurs, unités de stockage, imprimantes, etc.).

Compte tenu de son rôle central dans la politique de gestion des accès au sein d'une organisation, il constitue une cible de choix pour les attaquants.

L'obtention d'un accès administrateur sur cet annuaire entraîne une prise de contrôle instantanée des ressources ainsi gérées.

L'analyse des modes opératoires des récentes attaques met en évidence une recrudescence du ciblage des annuaires, compte tenu de leur importance dans le système d'information.

En effet, l'attaquant ayant obtenu des droits élevés sur l'annuaire peut alors déployer une charge malveillante. Par conséquent, le faible niveau de sécurité des annuaires met en danger les systèmes d'information dans leur globalité et fait porter un risque systémique aux organisations.

Il est donc nécessaire que chaque établissement de santé revoie la structure des annuaires Active Directory afin de viser une architecture dite « tiers ». Par la suite, il convient d'analyser les vulnérabilités logicielles et structurelles de cet annuaire grâce à un outil dédié à l'instar d'ORADAD.

Développé par l'ANSSI, le service ADS (Active Directory Security) met à disposition des opérateurs règlementés et de la sphère publique une capacité d'audit des annuaires Active Directory visant à leur donner de la visibilité sur le niveau de sécurité de leur annuaire. Les établissements de santé doivent appréhender les différentes mesures de contrôle et mettre en œuvre une politique d'amélioration continue de la sécurité des annuaires.

Enfin, l'annuaire doit faire l'objet d'une politique de sauvegarde particulière.

Le CERT Santé propose également un support permettant de guider les équipes chargées de la sécurité des système d'information dans leur démarche de durcissement de leur système d'information, et des annuaires en particulier.

Fiche réflexe 1 : maîtriser son système d'information

Désigner un responsable de la sécurité des systèmes d'information

- Évaluer la possibilité de mutualiser son intervention au sein du GHT
- Interlocuteur privilégié sur le périmètre de la cybersécurité

Impliquer le département informatique dans les processus d'acquisition

- Acquisition des dispositifs médicaux connectés
- Application des principes du « *privacy by design* » dans la gestion de projet

Sensibiliser le personnel

- Organiser une action de sensibilisation dans le programme de formation
- Organiser des exercices et simulation de problèmes informatiques

Réaliser et tenir à jour des cartographies du système d'information

- Repérer les matériels, logiciels, connexions réseaux
- Evaluer et repérer la criticité des systèmes d'information
- Repérer les serveurs stockant des données sensibles
- Repérer les composants du système d'information hors schéma directeur
- Définir l'ordre de priorité de remise en service des applications métiers
- Repérer les connexions avec les systèmes d'information externes
- Repérer les opérateurs de télémaintenance
- Limiter les accès à la cartographie du système d'information, confidentialité
- Mettre à jour régulièrement la cartographie

Effectuer une analyse des risques du système d'information

- Identifier les menaces potentielles et leurs impacts
- Évaluer les vulnérabilités des applications métiers critiques
- Évaluer les vulnérabilités de l'annuaire central
- Évaluer les défaillances potentielles d'un prestataire externe
- Évaluer les vulnérabilités liées au partage des données inter-établissements
- Évaluer les vulnérabilités des opérateurs de télémaintenance
- Évaluer la vulnérabilité des dispositifs connectés et des outils collaboratifs
- Hiérarchiser les mesures de protection en fonction des vulnérabilités
- Intégrer le processus cumulatif de dysfonctionnement
- Anticiper la mise en œuvre de contres mesures immédiates et évaluer l'impact

CHAPITRE 2 : FORMALISER UN PLAN DE MISE EN CONFORMITE ADAPTE

1. Formaliser des actions pour sécuriser le système d'information

1.1 Les directives NIS : sécurité des réseaux et des systèmes d'information

La directive « Network and Information System Security : NIS » a été adoptée par les institutions européennes le 6 juillet 2016. Cette directive est le premier élément de la législation européenne de cybersécurité et a pour objectif d'assurer une sécurité élevée commune pour les réseaux et les systèmes d'information de l'Union européenne. Elle définit des mesures concernant la sécurité des réseaux et des systèmes d'information européens. Elle s'applique particulièrement aux opérateurs de services essentiels (OSE) et aux fournisseurs de services numériques (FSN).

Inscrit en droit français par la loi de transposition du 27 février 2018 et par le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des Opérateurs de Services Essentiels, elle impose des obligations aux 135 établissements de santé supports de GHT. Cette directive visait à harmoniser et à renforcer la cybersécurité du marché européen.

Une nouvelle directive relative à la sécurité des réseaux et des systèmes d'informations, dite « NIS 2 » renforce les exigences en matière de cybersécurité et élargit les objectifs et le périmètre des secteurs concernés par des obligations de cybersécurité. L'un des plus grands changements imposés par la directive « NIS 2 » concerne les obligations de signalement des incidents.

1.2 La politique de sécurité des systèmes d'information (PSSI)

Chaque établissement doit rédiger un document spécifique relatif à sa Politique de Sécurité des Systèmes d'Information (PSSI). Cette PSSI nécessite au préalable un engagement formel de la direction de l'établissement. Une mutualisation des PSSI sera privilégiée au sein du GHT afin d'assurer une convergence des systèmes d'information.

En effet, l'arrêté du 1er octobre 2015 rend opposable la politique de sécurité des systèmes d'information aux établissements de santé publics et privés ainsi qu'à leurs prestataires et fournisseurs intervenant sur leur système d'information : périmètre informatique, biomédical, technique (GTB, GTC) et tout composant comportant de l'informatique embarquée.

L'instruction dite « 309 » (SG/DSSIS/2016/309) précise les éléments relatifs à l'obligation pour les établissements de santé de mettre en place un plan d'action SSI : Sécurité des Systèmes d'Informations.

L'Agence du Numérique en Santé (ANS) est chargée de l'élaboration et la publication de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), cadre devant être respecté par tous les acteurs de la santé pour sécuriser les systèmes d'information de santé (SIS).

1.3 Le plan d'action de sécurité des systèmes d'informations

Au regard de l'analyse de risque effectuée, il est recommandé de formaliser un plan d'action de sécurité des systèmes d'informations de l'établissement.

Pour les établissements de santé composés de plusieurs sites géographiques, il pourra être réalisé pour chacun des sites des plans d'action distincts mais disposant d'un socle commun.

Il sera nécessaire d'associer l'ensemble des prestataires extérieurs pour fiabiliser ce plan.

Ce plan d'action devra être révisé chaque année et notamment suite à une opération de réhabilitation/restructuration.

Ce plan décrira les mesures concrètes à mettre en œuvre avec un calendrier précis, intégrant des objectifs intermédiaires à atteindre et la répartition des actions entre les acteurs internes.

Il devra être adapté à chaque activité de soins ou activité support et précisera à la fois des mesures globales et des mesures ciblées.

Pour chaque mesure/action, il sera important d'en fournir une description, le nom du service ou de la personne responsable, le calendrier et d'en préciser le niveau d'avancement en pourcentage.

1.4 Les 23 règles de sécurité des 135 établissements supports de GHT

Les 135 établissements supports de GHT disposent du statut d'Opérateurs de Services Essentiels (OSE). De ce fait, ce statut implique quatre obligations pour ces établissements :

- L'application des 23 règles de sécurité aux systèmes d'information essentiels ;
- La désignation d'un point de contact à l'ANSSI ;
- La déclaration des systèmes d'information essentiels à l'ANSSI ;
- La notification à l'ANSSI des incidents de sécurité survenus sur les SIE.

L'arrêté du 14 septembre 2018 précise notamment des règles de sécurité numérique qui s'appliquent à ces 135 établissements de santé supports de GHT. Ces 135 établissements de santé devront garantir un socle minimal de cybersécurité pour se protéger d'une attaque aux conséquences majeures.

1.5 Définir les systèmes d'information essentiels

Ces 135 établissements supports de GHT ont notamment l'obligation de désigner auprès de l'ANSSI, les systèmes d'information essentiels de leur architecture interne - c'est-à-dire les systèmes d'information sur lesquels un incident de sécurité (indisponibilité prolongée, perte d'intégrité, défaut de confidentialité) aurait un effet disruptif important sur la prise en charge des patients. L'identification des systèmes d'information essentiels s'effectue dans le cadre d'une démarche générale d'analyse des risques.

Le décret n° 2018-384 du 23 mai 2018 précise que sont à prendre en compte les services concourant notamment aux activités de prévention, de diagnostic ou de soins, à la réception et à la régulation des appels, le service mobile d'urgence et de réanimation dans le cadre de l'aide médicale d'urgence, ainsi que la distribution pharmaceutique.

2. Des mesures prioritaires à mettre en œuvre

2.1 Le référentiel des 43 mesures prioritaires de sécurité des systèmes

Le référentiel des 43 mesures prioritaires de sécurité des systèmes d'information (MPR) à destination de l'ensemble des établissements de santé a été élaboré collégialement avec l'atelier sécurité des systèmes d'information, dans le cadre de la composition du référentiel MATURIN'H, et avec le club des responsables de sécurité des systèmes d'information des établissements de santé.

Le recueil des mesures est réalisé de manière déclarative au travers du dispositif de renseignement de l'Observatoire Permanent de la maturité SSI des établissements (OPSSIES) : outil de déclaration de conformité des établissements de santé aux différentes mesures de la plateforme oSIS.

Le recueil des mesures contribue également au pilotage : le suivi régulier de leur degré d'application concourt à une meilleure gouvernance à l'échelle hospitalière, régionale et nationale, permettant à tous d'améliorer la maturité SSI du système de santé.

Ces mesures sont décrites dans le référentiel à destination des établissements élaboré par la DGOS et disponible sur le site internet du ministère de la Santé et de la Prévention.

2.2 La gestion des correctifs de sécurité, une mesure prioritaire majeure

Les vulnérabilités non corrigées des applications et systèmes utilisés au sein d'un établissement peuvent être exploitées pour pénétrer le système d'information ou favoriser la propagation de celle-ci. Il est donc nécessaire de formaliser une démarche qui vise à effectuer les mises à jour de sécurité régulières sur les applications utilisées pour permettre de réduire le risque d'intrusion.

Par ailleurs, assurer une veille permanente via le CERT-FR et le CERT-SANTE permettra de rester informé de la découverte des vulnérabilités logicielles et matérielles des services utilisés dans votre établissement et de la disponibilité des correctifs.

Pour aller plus loin, consultez le document « Gestion des correctifs CER ».

2.3 Cloisonner l'architecture, une mesure prioritaire majeure

Il est important, dès la conception de l'architecture réseau, de raisonner par segmentation en zones composées de systèmes devant répondre à des conventions de sécurité homogènes. En effet, sans mesure de protection et à partir d'une seule machine infectée, une attaque peut se propager sur l'ensemble du système d'information, infecter la plupart des actifs accessibles et faciliter la prise de contrôle d'une multitude de ressources.

Pour limiter le risque de propagation, il convient d'effectuer une segmentation des différents éléments du système d'information par zones de sensibilité et d'exposition, par la limitation des privilèges accordés aux utilisateurs ou encore par la maîtrise des accès à Internet.

On pourra regrouper distinctement des serveurs d'infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc. Par exemple, un cloisonnement des niveaux d'administration peut être mis en place afin de s'assurer que les niveaux d'administration les plus élevés soient difficilement atteignables par les attaquants.

2.4 Maîtriser l'authentification des accès et des mots de passe

Le système d'information hospitalier doit répondre à un double enjeu de partage et de protection des données. Une politique de gestion des accès nécessite d'être formalisée pour caractériser pour chaque opérateur le degré d'ouverture des contenus, en consultation, en création, en modification et en suppression.

Enfin, le système d'information pouvant ne pas être administré exclusivement par des équipes infra-hospitalières, il est essentiel de s'assurer de la bonne gestion des accès accordés aux tiers, en charge par exemple du support à distance de composants critiques.

La revue complète des comptes et des habilitations est une opération à effectuer idéalement au moins une fois par an.

Une procédure de renouvellement automatique des mots de passe utilisateurs et administrateurs tous les 6 mois doit être mise en place.

Une authentification à deux facteurs pour les applications critiques est recommandée.

2.5 Protéger la messagerie professionnelle

La messagerie est le principal vecteur d'infection du poste de travail et d'intrusion dans le système d'information hospitalier, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site malveillant.

De surcroît, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d'informations de l'entité.

Les utilisateurs doivent être particulièrement sensibilisés à ce sujet. Un système d'affichage devra être proposé pour rappeler aux personnels les cyber-gestes.

A chaque nouvelle arrivée, un rappel des mesures de sécurité numérique sera proposé.

2.6 Des campagnes aléatoires de « *phishing* »

Des campagnes aléatoires de « *phishing* » pédagogiques sont un levier puissant pour la sensibilisation pour permettre de mesurer le niveau de maturité des personnels.

Au regard des résultats, des actions renforcées de sensibilisation et de formation pourront être nécessaires.

2.7 Identifier les données sensibles et les flux stratégiques

Compte tenu de la sensibilité et la confidentialité des données des établissements, il est indispensable de les repérer pour les protéger efficacement afin qu'elles ne puissent être rendues publiques.

À partir de cette liste de données sensibles, il sera possible de déterminer leur localisation au sein du système d'information afin de définir les mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation, les accès, etc.

Il convient aussi de passer en revue l'ensemble des flux de données sensibles, comprendre de quelle manière elles circulent au sein de l'établissement et à l'extérieur afin d'identifier les vulnérabilités potentielles et les risques de sécurité.

Ce processus permet de comprendre qui consulte et partage des informations personnelles ou sensibles dans l'établissement, qui en reçoit, quelles informations sont collectées, qui les conserve et qui y a accès.

2.8 Le référentiel Identifiant National de Santé : INS

Le référentiel Identifiant National de Santé (INS) décrit les conditions et modalités de mise en œuvre de l'obligation de référencement des données de santé. Afin de protéger les données de santé, l'identité INS est restreinte à un nombre limité d'acteurs. Pour ces acteurs, le référencement des données de santé avec l'identité INS est obligatoire.

Pour aller plus loin : Le référentiel national de santé

2.9 La nécessité de mettre en œuvre des audits réguliers

Il est demandé aux établissements de santé de procéder à des audits réguliers du système d'information pour permettre d'identifier les vulnérabilités et de proposer des mesures correctives. Il s'agit notamment d'évaluer les éléments suivants :

- Exposition de vulnérabilités sur internet : le « service de cybersurveillance » porté par le CERT santé de l'Agence du numérique en santé (ANS) permet de réaliser cet audit à distance ;
- La sécurité de l'Active Directory : service ADS de l'ANSSI permet de réaliser cet audit à distance via l'outil de collecte ORADAD fourni par l'ANSSI ;
- Le dispositif organisationnel : un audit organisationnel permet de mesurer pour l'établissements de santé la maturité de la gouvernance, de contrôler la prise en compte de la sécurité au niveau organisationnel sur la gouvernance, les procédures de sécurité.

Fiche réflexe 2 : un plan de mise en conformité

- Mettre en œuvre le décret 2018 pour les OSE : sécurité des systèmes d'information
- Formaliser un plan de mise en conformité conforme à la PSSI
- Appliquer l'instruction dite « 309 »
- Suivre et mettre en œuvre les correctifs de sécurité
- Cloisonner l'architecture du système d'information
- Mettre en œuvre le référentiel des 43 mesures prioritaires
- Mettre en œuvre les 23 règles pour les établissements support de GHT
- Identifier les systèmes d'information essentiels
- Maîtriser les accès et les mots de passe du système d'information
- Protéger la messagerie professionnelle du personnel
- Réaliser des campagnes de « *phishing* »
- Maîtriser et sécuriser les données sensibles de l'établissement
- Mettre en œuvre le référentiel national de santé INS
- Assurer une veille : CERT-FR /CERT-SANTE sur les vulnérabilités logicielles
- Réaliser des audits réguliers du système d'information

PARTIE 2 : ELABORER LE VOLET NUMERIQUE

CHAPITRE 1 : LES MODALITES DE MISES EN ŒUVRE

1. L'articulation avec les plans ORSAN, Gestion des tensions, PCA, PRA

1.1 Le plan ORSAN : un plan de réponse régional

Le dispositif régional « ORSAN » constitue le cadre intégré de préparation et de réponse aux situations sanitaires exceptionnelles du système de santé et organise la montée en puissance des professionnels de santé et des opérateurs de soins sous la coordination et le pilotage régional de l'ARS.

Il permet d'assurer la réponse sectorielle sanitaire et s'articule avec le dispositif intersectoriel ORSEC, élaboré sous l'autorité des préfets, notamment pour garantir la continuité des parcours de soins des patients.

Le plan ORSAN est déclenché par le directeur général de l'ARS, le cas échéant, à la demande du préfet ou du ministre chargé de la santé, il est décliné par les établissements de santé dans leur plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, en fonction des objectifs capacitaires de prise en charge fixés par l'ARS en fonction de leur plateau technique (première ligne, deuxième ligne ou troisième ligne).

Le dispositif régional « ORSAN » prend en compte, dans la Disposition Spécifique Transversale (DST) « cybersécurisation des établissements sanitaires », le risque numérique comme une menace pesant sur les systèmes d'information et comme un risque majeur pour le fonctionnement des établissements de santé et la prise en charge des patients. A ce titre, l'ARS est en charge de la coordination de la réponse territoriale à un incident de nature « cyber ».

Il est donc nécessaire de le décliner par des mesures opérationnelles, dans le cadre de l'élaboration du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles des établissements de santé.

1.2 Le plan de gestion des tensions hospitalières

Le plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles vise à adapter rapidement les organisations internes de chaque établissement pour notamment mobiliser leurs ressources dès lors qu'un événement vient perturber le fonctionnement normal de l'établissement.

Le directeur de l'établissement décide de l'activation de l'un des deux niveaux de réponse du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles :

→ Niveau 1 : Plan de mobilisation interne
- Pour la gestion des tensions ou des situations avérées potentiellement critiques, sans toutefois mettre à court terme, l'établissement en difficulté dans son fonctionnement courant (épidémie saisonnière…).

→ Niveau 2 : Plan blanc
- Pour la gestion des situations exceptionnelles avec un impact potentiellement majeur sur l'établissement de santé. Il permet d'assurer la prise en charge des patients lors d'événements graves et/ou inhabituels tout en maintenant la continuité et la qualité des soins (attentat, crise épidémique, cyberattaque, incendie, séisme…)

Chaque établissement de santé doit décliner au sein du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, un volet spécifique au risque numérique.

Ce guide d'aide à la préparation du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles s'inscrit dans la déclinaison du dispositif régional ORSAN et de la disposition spécifique transversale « cybersécurisation des établissements sanitaires ».

Ce volet numérique décrit les mesures graduées activables en fonction de la nature, de l'ampleur et de la cinétique de l'incident numérique.

1.3 L'articulation avec les plans de continuité/reprise d'activité

Le volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles décrira le cadre de réponse général et précisera les séquences à suivre lors d'un incident numérique majeur.

Chacune des séquences sera mise en œuvre selon un ordonnancement précis.

Les étapes relatives à la « continuité d'activité » et à la « reprise d'activité » du système d'information s'effectueront conformément aux procédures décrites dans :

→ Le « plan de continuité d'activité du système d'information - PCA » :
- Vise à maintenir la continuité d'activité du système d'information ;
- Décrit l'architecture de secours du système d'information en cas de panne ou de cyberattaque ;
- Décrit les modalités de bascule qui viseront à maintenir de façon immédiate et sans interruption, la continuité de fonctionnement des composants majeurs du système d'information.

→ Le « plan de reprise d'activité du système d'information - PRA » :
- Les modes opératoires (procédures détaillées conformément aux préconisations du fabricant) pour restaurer à partir des sauvegardes réalisées chacune des applications métiers ou autres composants majeurs du système d'information.

1.4 Le plan de continuité d'activité du système d'information : PCA

Le « plan de continuité d'activité du système d'information - PCA » vise à maintenir l'activité de l'établissement de santé lors d'un incident numérique. Il décrit l'architecture de secours du système d'information pour permettre de maintenir en condition opérationnelle les activités de production informatique et de support de l'établissement.

Ce plan qui est aussi nommé « Plan de continuité informatique - PCI » est un sous-ensemble du PCA global de l'établissement de santé, le PCI étant sa déclinaison sur le volet informatique. D'usage, le terme PCI est peu utilisé. On évoque le plus souvent « PCA du système d'information ».

Le PCA du système d'information décrit notamment :

→ <u>L'infrastructure de secours, il s'agit par exemple du :</u>

- Dédoublement de la salle machine « environnement de production » au sein d'une salle de secours ou salle dite « miroir ». Ce mode permet de reconstituer l'environnement de production et de transférer de façon quasi immédiate la production sur les plates-formes de secours ;
- Dédoublement du cœur de réseau, serveur redondé ;
- Dédoublement des lignes de connexion par des chemins de câble distincts ;
- Les modes de bascule vers ces solutions de secours. En effet, dans la mesure du possible, il convient que l'infrastructure automatise au maximum la réponse à une panne, telle que la bascule automatique d'un élément technique vers le second élément technique de secours.

→ <u>Les procédures dégradées :</u>

- L'ensemble des procédures dégradées nécessaires au maintien en condition opérationnelle des activités de production informatique et de support lors de la survenue d'une avarie sur un élément fonctionnel majeur du système d'information. Par exemple, pour chacune des applications métiers utilisées, une procédure détaillée décrira les actions à réaliser et notamment l'activation du « mode dégradé » de l'application. En effet, de nombreuses applications métiers disposent d'un fonctionnement « mode dégradé » qui permet de garantir la continuité de fonctionnement en cas d'avarie sur le système d'information de l'établissement.

1.5 Le plan de reprise d'activité du système d'information : PRA

Le « plan de reprise d'activité du système d'information - PRA » définit les processus à mettre en œuvre pour restaurer les équipements et les applications métiers corrompus.

Ce plan, aussi nommé « Plan de reprise informatique - PRI », est un sous-ensemble du PRA général de l'établissement, le PRI étant sa déclinaison sur le volet informatique. D'usage, le terme PRI est peu utilisé. On évoque le plus souvent « PRA du système d'information ».

Le PRA du système d'information décrit notamment :

- Les procédures détaillées formalisées en lien avec le fabricant, qui permettront la restauration de chacun des éléments du système d'information corrompus ;
- Les procédures de restauration des machines virtuelles depuis une sauvegarde totale ;
- Les procédures de restauration d'équipements, de données ou base de données ou logiciel/application depuis une sauvegarde.

2. Le volet numérique

2.1 L'intérêt de disposer d'un volet numérique

Lors d'une crise numérique, le fonctionnement nominal des applicatifs métiers du système d'information de l'établissement peut être dégradé, voire inopérant. Le risque de cyberattaque étant une réalité, il est nécessaire de prendre des mesures en amont et adopter des stratégies de défense en adéquation avec le paysage actuel des menaces.

Il est nécessaire d'anticiper la formalisation d'un volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles.

Ce travail de préparation porté par les équipes de la direction des systèmes d'information, mais aussi des services de soins de l'établissement, permettra de limiter les impacts d'un incident numérique et notamment d'une cyberattaque et de rétablir un fonctionnement normal dans un délai acceptable.

Il sera nécessaire d'adapter le volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles au type d'établissement. En effet, les réponses à une cyberattaque varient selon la taille, la présence de services critiques, le type de plateau technique, les processus logistiques d'approvisionnement et les applicatifs externalisés. De ce fait, l'élaboration et la mise en œuvre des mesures de gestion en cas d'incident seront très différentes entre un centre hospitalier régional et une structure de soins qui assure des soins au sein d'une unité de soins de longue durée.

Ces éléments de préparation permettront d'engager des mesures proportionnées et adaptées dès l'identification de l'incident.

2.2 Un volet numérique qui pourra être mutualisé au sein du GHT

Les éléments de préparation du volet numérique pourront être mutualisés au sein d'un GHT ou au niveau régional pour permettre une appropriation par le plus grand nombre et une stratégie unique.

Cette mutualisation pourra s'effectuer en lien avec l'ARS et le GRADeS.

2.3 Les critères de déclenchement du volet numérique

Le déclenchement du plan blanc numérique n'est pas systématique en cas d'incident sur le système d'information.

C'est la compromission des applicatifs essentiels de l'établissement et notamment la durée prévisionnelle d'indisponibilité avec un risque de perte de chance pour les patients pris en charge qui traduira le déclenchement du plan blanc numérique, à la discrétion du directeur de l'établissement.

Il s'agira en fonction du résultat des éléments d'investigation et notamment la gravité de l'incident et sa durée prévisionnelle, d'arbitrer le déclenchement du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles.

2.4 La confidentialité du volet numérique

Le volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles peut être considéré comme confidentiel, voire stratégique, pour les établissements de santé disposant du statut d'opérateurs de services essentiels (OSE), car il dévoile les détails de la réponse face à un incident numérique et notamment une cyberattaque.

Certaines informations et modalités de mise en œuvre du volet numérique doivent être protégées, notamment pour ne pas permettre leur exploitation par des personnes malveillantes.

Autant, il est nécessaire de communiquer en interne pour fédérer l'ensemble des professionnels de santé et des personnels de l'établissement, autant les détails de ce volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles doivent, pour certains aspects, conserver une part de confidentialité.

Des clauses contractuelles de confidentialité devront être formalisées en amont de l'intervention d'équipes d'intervention externes sur le système d'information de l'établissement de santé.

D'un point de vue général, c'est l'architecture de sécurité du système d'information et de ses différents composants de sécurité qui devra être protégée.

3. Coordonner et impliquer l'ensemble des acteurs

3.1 L'implication des acteurs pour l'élaboration du plan

Afin de disposer d'une organisation adaptée au sein de l'établissement, il est nécessaire de réunir en amont de la crise un groupe chargé de la planification.

Ce dernier devra réunir, a minima, l'équipe chargée de la sécurité des systèmes d'information de l'établissement, la commission « situations sanitaires exceptionnelles - SSE », des représentants des personnels médicaux et paramédicaux concernés avec l'implication effective de la direction d'établissement, du président de la CME, de la direction des soins infirmiers, de représentants des services financiers, des représentants des ressources humaines, du comité d'hygiène, de sécurité et des conditions de travail (CHSCT), du coordonnateur de la gestion des risques associés aux soins, de l'équipe opérationnelle d'hygiène (EOH), ainsi que des services techniques et logistiques.

Il s'agira notamment d'élaborer des procédures pour faire face à un potentiel incident, d'organiser la formation et l'entraînement des personnels impliqués dans la gestion de crise.

Des aspects logistiques concernant notamment la continuité des approvisionnements et de la gestion des ressources humaines seront également à prendre en compte.

3.2 La coordination par l'ARS en lien avec le GRADeS

Dans le cadre des éléments de préparation à une cyberattaque, il est nécessaire de définir des modalités de coordination et d'appui régionaux avec les établissements du bassin territorial, que ce soit en matière de continuité des soins ou en matière de mutualisation des compétences techniques.

L'ARS pourra déclencher en fonction de la gravité de l'évènement, sa cellule régionale d'appui au pilotage sanitaire (CRAPS) conformément au dispositif ORSAN régional de préparation et de réponse à une situation sanitaire exceptionnelle. Cette coordination doit être prévue et permettre l'accueil de nouveaux patients en cas d'impossibilité temporaire d'assurer des prises en charge pour l'établissement attaqué.

La coordination des ressources techniques spécialisées disponibles et de la prise en charge médicale des patients entre établissements en cas de cyberattaque est faite par l'ARS, en lien avec le GRADeS régional (groupement régional d'appui au développement de la e-santé).

Le GRADeS pourra accompagner les établissements de santé sur les thèmes relatifs à la sécurité numérique et la protection des données personnelles. Il pourra mettre à disposition des outils commun de sensibilisation, proposer des méthodes d'analyse des risques, effectuer une veille sur les menaces et les vulnérabilités, organiser au niveau régional des campagnes de « *phishing* », proposer des tests d'intrusion et des audits sur la vulnérabilité des systèmes d'information. Son action visera à accompagner les établissements de santé et notamment d'évaluer en lien avec l'établissement de santé, la nécessité de contractualiser avec un Prestataire de Réponse à Incident de Sécurité (PRIS) disponible 24h/24.

3.3 Un appui des agences nationales : ANS, ANSSI

Dans le cadre de la gestion de crise et notamment dans l'évaluation du niveau de gravité de l'incident, l'établissement pourra s'appuyer sur les compétences de l'agence du numérique en santé (ANS).

En effet, l'ANS joue un rôle central, en particulier grâce au CERT Santé qui accompagne les établissements de santé dans la veille sur les menaces de cybersécurité et la réponse à un incident de sécurité des systèmes d'information. L'ANSSI pourra aussi apporter un appui important en fonction de la gravité de l'incident.

4. Une cellule de crise : décision et opération

4.1 Un organe de pilotage de la crise numérique

Une cellule de crise hospitalière doit être mise en place dès le déclenchement d'un des deux niveaux du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles (PGTHSSE) développé pour les établissements de santé.

Une crise de type cyberattaque entrainant une désorganisation de l'offre de soins nécessite d'être traitée à deux niveaux : décisionnel et opérationnel.

Le dispositif de crise à établir se composera :

→ <u>D'un volet décisionnel :</u>

Le volet décisionnel réunira notamment la direction générale de l'établissement, le directeur médical de crise (DMC), le responsable de la sécurité des systèmes d'information et le président de la CME (commission médicale d'établissement).

Il vise à :

- Organiser la communication interne et externe sur l'incident en cours ;
- Organiser le travail des différents services des soins ;
- Réorienter les patients et les professionnels de santé si nécessaire ;
- Déterminer l'ordre dans lequel les services seront rendus opérationnels ;
- Mobiliser les ressources nécessaires à la résolution de l'incident.

Ce volet décisionnel pourra comporter 7 pôles conformément à ses 7 missions : situation/coordination, décision, organisation de la prise en charge médicale, fonctions support, sûreté/sécurité, accompagnement des familles, communication. Un pôle « anticipation » et « retour au fonctionnement normal » pourra être mis en place en fonction de la situation.

Cette cellule devra établir un mode de communication adéquat afin que l'ensemble des participants possèdent le même niveau d'information en temps réel.

→ D'un volet technique opérationnel :

Le pôle « technique opérationnel » réunira les compétences techniques de l'établissement : informatique, biomédicale, technique et logistique. Ce pôle pourra être complété par des profils experts des agences régionales et nationales (ANS, ANSSI) et si nécessaire, par un représentant du prestataire « réponse à incident » lorsqu'il est sollicité. Ce pôle vise à piloter et notamment à mettre en œuvre les opérations suivantes : détection, confinement, conduite des étapes d'éradication ; restauration et reconstruction si nécessaire ; production d'états d'avancement de ces travaux au pôle décision.

4.2 La désignation d'un directeur médical de crise DMC

Lors de l'activation du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, un directeur médical de crise (DMC) est désigné par la direction générale afin notamment d'organiser les flux de patients en lien avec la cellule de crise hospitalière sous l'égide du directeur général et du président de la commission médicale d'établissement.

4.3 Le rôle de la cellule de crise hospitalière

La cellule de crise hospitalière est principalement chargée de :

- Centraliser l'ensemble des informations techniques ;
- Mesurer l'impact sur la prise en charge médicale et sur la capacité à l'établissement à assurer la prise en charge de nouveaux patients ;
- Valider les actions à mettre en œuvre pour permettre la continuité de l'activité.

Elle est en contact permanent avec le correspondant de l'ARS, ainsi que le SAMU-Centre 15 territorialement compétent par l'intermédiaire du DMC.

Un dispositif de suivi et de synthèse des actions en cours doit être partagé au sein de la cellule de crise par le pôle situation/coordination.

Un journal de crise, horodaté et signé, rendant compte des caractéristiques de l'incident, des moyens mis en œuvre et de l'efficacité du plan de crise doit être rédigé. Tout changement notable de la situation justifie un point de situation succinct qui doit être transmis par écrit aux autorités de tutelle et au SAMU-Centre15.

La cellule de crise doit être adaptée à la nature de l'intrusion pour faire face à une cyberattaque. La sollicitation d'un représentant de l'équipe « réponse à incident » et de personnes expertes internes/externes à l'établissement peut s'avérer capital. Il s'agira alors de l'inclure dans la cellule de crise hospitalière.

Un responsable de l'organisation de la cellule de crise sera désigné. Il sera chargé de la gestion de la coordination de la cellule et de ses membres et de la prise de décisions.

Une liste des membres (vivier) susceptible de constituer la cellule de crise sera établie et devra disposer des informations suivantes : coordonnées professionnelles et privées des personnes désignées (nom, prénom, fonction, téléphone, courriel). Ces informations sont récoltées, stockées de manière sécurisée et consultables selon le règlement sur la protection des données personnelles.

La direction de la cellule de crise hospitalière pourra être amenée à communiquer au grand public et aux éventuels médias présents sur l'événement. Il est nécessaire d'assurer cette communication en respect de la stratégie de communication de l'ARS et, le cas échéant, de la Préfecture.

Pour aller plus loin, le guide « crise d'origine cyber – les clés d'une gestion opérationnelle et stratégique » publié par l'ANSSI.

4.4 La cellule de crise hospitalière communique régulièrement en interne

Des informations régulières de la cellule de crise nécessite d'être transmises aux différents pôles de l'établissement de santé pour que ceux-ci disposent d'une visibilité essentielle. Ces informations permettront aussi de mettre en œuvre les modalités de fonctionnement dégradé les plus pertinents au sein des différents services.

4.5 La logistique nécessaire à une cellule de crise

La cellule de crise devra être dotée de moyens lui permettant de remplir sa mission sur toute la durée nécessaire.

La salle sera dotée d'un dispositif de connexion internet qui permettra d'être secouru en cas de coupure interne, de lignes téléphoniques fonctionnelles même en cas d'avarie sur le réseau principal et notamment d'un procédé de messagerie interne en cas d'indisponibilité.

Une cyberattaque pourra aussi restreindre les capacités de communication internes et parfois externes. Il sera alors nécessaire de prévoir des moyens de communication spécifiques pour assurer la gestion de crise et garantir la continuité des échanges d'information.

Il faut également faciliter le partage, en mode déconnecté, de l'annuaire téléphonique des instances de gouvernance et des services tiers des autres établissements du GHT.

4.6 Un vecteur de communication rapide et sécurisé

Il est recommandé d'évaluer la nécessité de prévoir une organisation de « communication rapide » via une application externe de type « groupe » pour permettre des échanges d'information rapides et sécurisés entre les membres de la cellule de crise. Bien entendu, il est utile de rappeler l'interdiction de communiquer des informations couvertes par le secret médical/professionnel via des vecteurs de communication non sécurisés.

5. La mobilisation de ressources techniques expertes

5.1 Des ressources techniques d'intervention

Dans le cadre du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, il est essentiel de préparer en amont les moyens opérationnels adaptés aux *scenarii* de crise. Il s'agira de disposer d'une équipe technique dédiée qui pourra être mobilisée dès les premières heures de l'attaque.

Cette équipe aura pour objectif de minimiser l'impact de la crise et d'assurer la restauration rapide des processus affectés et de mettre en œuvre des mesures de prévention pour éviter un évènement similaire.

Il sera nécessaire de tenir à jour une liste des personnes ressources internes et externes à l'établissement et de prévoir, le cas échéant, leur mobilisation rapide grâce à des listes qui devront être tenues à jour régulièrement.

5.2 Une équipe « réponse à incident » mutualisée au sein du GHT

En lien avec les services de l'ARS et de son GRADeS, il pourra être possible, compte tenu de la spécificité des compétences requises, de mutualiser les ressources techniques existantes, dédiées à la sécurité des systèmes d'information au sein des établissements du GHT ou de la région.

Ces référents « réponse à incident » déjà positionnés au sein d'établissements du GHT, pourraient en cas de nécessité, intervenir dans un délai court, pour renforcer l'équipe locale d'un établissement.

Des travaux de préparation devront bien entendu être réalisés par cette équipe restreinte « réponse à incident » pour disposer des informations essentielles (cartographie…) sur les sites éventuels d'intervention.

Il sera nécessaire de bien définir le rôle et les missions affectés à chacun des membres de l'équipe.

Ainsi, des compétences pourraient être exclusivement chargées d'identifier l'origine de l'attaque, de détecter et préciser le périmètre de la compromission, d'effectuer les opérations de confinement et d'éradication. D'autres seraient plutôt chargées de réaliser les processus de restauration des sauvegardes et de la reconstruction des applications métiers corrompues. Enfin, des compétences seraient plutôt orientées vers l'accompagnement au fonctionnement en mode dégradé et notamment en cas d'incident majeur, à la constitution des infrastructures temporaires.

Dans l'impossibilité de disposer de l'expertise suffisante au sein de l'établissement, du GHT ou de la région, il est recommandé d'évaluer la possibilité de mobiliser des prestataires qualifiés par l'ANSSI (PRIS : Prestataires de réponse aux incidents de sécurité) ou à défaut d'ESN (entreprise de service numérique) en capacité d'appréhender les processus métiers hospitaliers, pour accompagner les équipes métiers dans leurs capacités de détection, d'investigation, de reconstruction et de gestion des impacts de la crise.

Un travail de pré-contractualisation peut être effectué en amont via des contrats-cadres ou des référencements à l'échelle du GHT ou de la région, en prenant en compte les compétences déjà représentées au sein du territoire.

Pour aller plus loin, la liste des Prestataires de réponse aux incidents de sécurité qualifiés par l'ANSSI.

5.3 L'appui de l'ANS et de l'ANSSI

Un accompagnement peut être sollicité auprès de l'ANSSI pour les établissement désignés OIV (opérateur d'importance vitale) ou OSE (opérateur de service essentiel) mais il dépendra toutefois des disponibilités de l'ANSSI en fonction notamment du nombre d'incidents simultanés tous secteurs confondus par exemple. Pour rappel, les établissements OSE sont les établissements supports de GHT.

Cet accompagnement pourra aussi être sollicité par les autres établissements de santé.

Les établissements désignés OSE ont l'obligation de disposer d'un point de contact avec l'ANSSI, et d'autre part, de déclarer préalablement les systèmes d'information essentiels de leur établissement à l'ANSSI.

Dans le cadre de la gestion de crise et notamment dans l'évaluation du niveau de gravité de l'incident, l'établissement pourra aussi s'appuyer sur les compétences de l'ANS. En effet, elle joue un rôle central, en particulier grâce au CERT Santé qui accompagne, selon ses disponibilités, les établissements de santé dans la veille sur les menaces de cybersécurité et la réponse à incident de sécurité des systèmes d'information.

Consultez l'observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social 2022

6. Les étapes à suivre lors d'un incident numérique

6.1 Des mesures de gestion adaptées à la nature de l'incident numérique

Les mesures de gestion à mettre en œuvre en cas d'incident numérique et notamment une cyberattaque sont perlées et nécessitent de mettre en œuvre une expertise dédiée pour chacune d'elles. Ces mesures devront être adaptées à la nature et la typologie de l'incident numérique.

Comme évoqué, cette expertise, si elle n'est pas disponible au sein de l'établissement pourra être mutualisée au sein du GHT ou de la région. Par exemple, l'étape de détection de l'intrusion nécessite des compétences et des outils spécifiques.

Selon le niveau de gravité et la rapidité de réaction, il pourra être nécessaire de réaliser uniquement les premières étapes : détection, qualification de l'incident, confinement, éradication.

Dans le cas contraire, il sera nécessaire de poursuivre le cheminement séquencé des actions à mettre en œuvre et dans le cas le plus défavorable, de reconstruire les composants corrompus.

- Détecter, identifier l'origine de l'intrusion, caractériser le périmètre de la compromission ;
- Qualifier la gravité de l'incident numérique ;
- Vérifier l'intégrité des sauvegardes ;
- Confiner et identifier les systèmes compromis ;
- Eradiquer les codes malveillants ;
- Engager et accompagner le fonctionnement en mode dégradé ;
- Créer des infrastructures temporaires, locales avec des systèmes de sauvegarde ;
- Restaurer les applications métiers ;
- Si nécessaire « reconstruire » les composants corrompus ;
- Arbitrer la fin de la crise numérique.

En fonction du niveau de gravité de l'incident, les mesures de gestion à mettre en œuvre devront prendre en compte les étapes à suivre prévues dans le « PRA du système d'information ».

L'ensemble de ces séquences vont être détaillées dans les éléments de préparation ci-après.

7. La conservation des preuves, le dépôt de plainte et la demande de rançon

7.1 La collecte des preuves des systèmes attaqués

Lorsqu'un établissement de santé est exposé à une cyberattaque, il est nécessaire de collecter des preuves des systèmes attaqués : fichiers de journalisation (logs) du pare-feu, serveur mandataire (proxy) et serveurs touchés, et les tenir à disposition des enquêteurs.

Au cours des investigations initiales, il est important de ne pas détruire les traces, les preuves qui seront nécessaires aux enquêteurs puisque chaque attaque doit donner lieu à un dépôt de plainte et généralement à un signalement à la CNIL car s'agissant des établissements de santé, les données personnelles sont généralement impactées.

Ces éléments peuvent permettre d'obtenir des « traces » du cybercriminel dans le cadre de l'analyse de l'attaque. L'établissement pourra en complément, signaler les faits via la plateforme de signalement « Pharos ».

Ces éléments peuvent constituer des preuves à valeur juridique en cas de procédures ultérieures.

Tout au long du processus de gestion de crise, il sera nécessaire de récolter au fur et à mesure les différents éléments de preuve tels que les journaux, les défauts d'accès des utilisateurs.

Par anticipation, il s'agira de disposer de support pour copier les éléments de preuve.

7.2 Le dépôt de plainte

À la suite d'une cyberattaque, il est nécessaire d'effectuer rapidement un dépôt de plainte auprès d'un service de Police nationale ou de Gendarmerie nationale (dans les 24 à 48h après la découverte de l'incident).

Il s'agira de recueillir au préalable les références de la (ou des) personne(s) contactée(s) si elles ont pris l'attache de l'établissement de santé : adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, copie des courriels ou courriers échangés ou tout autre renseignement pouvant aider à l'identification de l'attaquant.

7.3 La gestion de la demande de rançon

Vous ne devez pas négocier avec l'assaillant, seules des personnes expertes en la matières (force de l'ordre) peuvent le faire si elles le jugent utile.

Le paiement de la rançon est exclu, car il entretient le système frauduleux et ne garantit pas la récupération des données ou des systèmes compromis. De plus, le paiement de la rançon n'empêchera pas votre établissement d'être à nouveau la cible de cybercriminels. L'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés.

Le paiement de la rançon désigne la victime comme ouverte au paiement de rançon ce qui l'expose à une nouvelle attaque.

Fiche réflexe 3 : Modalités de mises en œuvre du volet numérique

- Élaborer un volet numérique
- Adapter le volet numérique à la nature de l'incident numérique
- Anticiper les mesures de gestion en fonction du type d'établissement
- Mettre en œuvre un volet numérique qui pourra être mutualisé au sein du GHT
- Corréler les mesures à mettre en œuvre avec le plan de continuité/reprise d'activité
- Se préparer au regard de l'impact sur l'offre de soins
- Définir des critères de déclenchement du volet numérique
- S'assurer de la confidentialité des mesures du volet numérique
- Impliquer la gouvernance interne à l'établissement pour l'élaboration du plan
- Organiser par anticipation la cellule de crise : membres, rôles et missions
- Organiser la logistique de la cellule de crise : téléphone, internet, liste des contacts
- Anticiper des moyens sécurisés de communication rapide type « groupe »
- Évaluer la possibilité de créer une équipe « réponse à incident »
- Définir le rôle/missions de l'équipe « réponse à incident »
- Définir des modalités de coordination avec l'ARS et le GRADeS
- Anticiper les échanges avec les experts nationaux (ANSSI, CERT-FR…)
- Anticiper l'appui de l'ANSSI et de l'ANS (liste des contacts)
- Anticiper les étapes à suivre pour restaurer un système d'information
- Anticiper la conservation des preuves, le dépôt de plainte

CHAPITRE 2 : LES ELEMENTS GENERAUX A PREPARER

1. Les éléments de préparation généraux

1.1 Des travaux d'anticipation

Le facteur majeur en cas de crise est la gestion du temps. L'anticipation est par conséquent indispensable.

L'imprécision initiale est réduite si l'on sait s'entourer d'emblée d'un plan de réponse, des moyens adéquats, d'un réseau de partenaires et de technologies de communication.

Il est difficile de pouvoir déterminer les caractéristiques précises d'une éventuelle intrusion par exemple. Face à cette incertitude, la démarche retenue visera dans un premier temps à développer un plan de réponse robuste.

Les travaux de préparation à un incident numérique traduisent non seulement des mesures de gestion à mettre en œuvre en cas de crise, mais caractérisent aussi les lacunes qui peuvent être comblées avant une situation de crise.

Un établissement doit donc élaborer une stratégie claire d'actions précises à mettre en œuvre après un incident confirmé, afin d'éviter la confusion, les retards inutiles et une mauvaise hiérarchisation des priorités.

Il sera nécessaire de faire le lien avec les travaux de préparation déjà engagés dans le cadre du plan de reprise d'activité du système d'information (PRA).

1.2 Une réponse adaptée aux principaux scenarii

La planification des mesures de gestion doit être formalisée au regard des *scenarii* basés sur des événements récents qui ont eu un impact sur d'autres établissements de santé, afin de développer des procédures adaptées. Réfléchir à chaque scenario aide un établissement à évaluer l'impact potentiel, les mesures à mettre en œuvre et les processus de récupération qui en résultent.

Ces différents *scenarii* aident également à prévoir les moyens techniques nécessaires et à adapter les ressources humaines.

L'analyse des *scenarii* possibles doit être formalisée en amont et régulièrement mise à jour au regard des cyberattaques récentes.

Compte tenu du nombre important de *scenarri*, le principe de précaution impose de se préparer aux évènements les plus probables mais aussi aux modalités d'organisation d'un incident numérique d'origine inédite.

Pour aller plus loin, un document de l'ANSSI sur la méthode EBIOS RM.

1.3 Une stratégie de réponse commune au sein du GHT ou de la région

Dans le cas des GHT, il convient de disposer d'une stratégie d'anticipation et de réponse commune entre tous les établissements du GHT.

La stratégie de réponse de l'établissement face à un risque numérique ou à une menace de cyberattaque, doit reposer sur les dispositifs de préparation et de réponse aux tensions hospitalières et aux situations sanitaires exceptionnelles préexistantes. Ces mesures opérationnelles doivent être testées par les équipes en charge des systèmes d'information.

Par exemple, la planification des mesures de gestion à mettre en œuvre et la documentation nécessaire pour permettre la restauration après une cyberattaque doivent être disponibles avant que l'événement ne se produise. Un socle commun pourra être partagé au sein des établissements du GHT

La crise numérique obéit globalement à la même cinétique que les autres crises liées à des risques physiques.

Les procédures de gestion des crises nécessitent d'être préétablies et testées.

1.4 Une description de l'offre de soins et des prises en charge à risque

Dans un contexte de crise, il s'agira pour une équipe dédiée et principalement composée de ressources médicales et paramédicales, dans le cadre du volet numérique de recenser, au préalable, les services hébergeant les patients à risque.

Il s'agira de disposer d'une procédure rapide permettant d'évaluer avec les professionnels de santé, les sorties anticipées des patients vers leur domicile ou une structure tierce, de disposer d'une procédure rapide pour étudier la pertinence d'annulation d'hospitalisations programmées, de disposer d'une procédure rapide qui permet d'identifier les patients dont l'hospitalisation ne peut être différé.

Cet état des lieux permettra de disposer de la localisation des prises en charge au sein de l'établissement et de vérifier si les modalités en fonctionnement dégradé sont suffisantes au regard des soins qui nécessitent d'être prodigués.

1.5 Un stock stratégique idéalement mutualisé

Le volet numérique doit identifier les moyens dont dispose l'établissement pour faire face à une situation sanitaire exceptionnelle.

Dans l'idéal, le plan de préparation doit prévoir, au-delà des ressources propres de l'établissement pour son fonctionnement normal, d'autres matériels et équipements pour assurer la reprise du système d'information. L'établissement de santé pourra en amont contractualiser avec un opérateur pour disposer, en cas de nécessité, et dans un délai restreint, des matériels et équipements nécessaires.

Ce stock stratégique doit être suffisant pour permettre de reconstruire une bulle sécurisée des applicatifs critiques indispensables au fonctionnement de l'établissement.

Ce stock de matériels qui pourra être idéalement mutualisé à l'échelle du GHT ou de la région, devra être facilement accessible et mobilisable 24/7.

1.6 L'obligation de réaliser des exercices

Un exercice de gestion de crise consiste à réaliser en amont de la survenue d'une situation réelle, des mises en situation avec les équipes concernées.

Un exercice se déroule sur une durée limitée, dans un contexte imaginé pour l'occasion et repose sur l'organisation de gestion d'une crise en place au moment où il est joué. Un exercice de gestion de crise ne doit en aucun cas avoir un impact réel sur les activités de l'établissement de santé.

L'objectif d'un exercice est de tester la cyber résilience de l'établissement de santé sur toute ou partie des organisations :

- La chaîne d'alerte et le dispositif de crise ;
- Les outils et les procédures existantes liés à la gestion des incidents et des crises ;
- La coordination entre la gestion des équipes cybersécurité et l'impact sanitaire ;
- La communication de crise interne/externe de la cellule de crise ;
- La coordination de la cellule de crise avec le niveau régional et les autorités ;
- La capacité des structures à travailler sans système d'information.

Il existe également des exercices opérationnels de gestion de crise : par exemple, il apparait utile d'entraîner les équipes en charge des systèmes d'information à restaurer un annuaire central, à rechercher des journaux d'événements, à gérer les règles du pare-feu pour couper une ou plusieurs parties du système d'information d'Internet. Ces exercices nécessitent d'être maitrisés par la direction des systèmes d'information afin d'augmenter la célérité de la prise en charge de la crise.

Pour aller plus loin, l'ANS propose des kits pratiques (débutant, intermédiaire, avancé) pour réaliser des exercices de crise.

Un guide de l'ANSSI précise les modalités de réalisation d'un exercice de crise.

1.7 Des tests d'intrusion pour évaluer la sécurité globale

Au-delà de l'exercice de crise, des tests d'intrusion sont un excellent moyen d'identifier les failles physiques et numériques. Ces tests d'intrusion ont pour but d'évaluer la sécurité globale du système d'information en mettant à l'épreuve ses différents moyens de protection, qu'ils soient physiques, humains, organisationnels et informatiques.

2. Les travaux préparatoires à la communication

2.1 Des outils de communication à préparer

L'information et la communication sont primordiales, notamment au regard du rôle joué par les médias et les réseaux sociaux.

Il est nécessaire de préparer en amont de toute crise des outils et des procédures pour pouvoir anticiper les réactions, les interrogations et les perceptions de l'ensemble des parties prenantes, ainsi que de communiquer de la manière la plus appropriée sur l'incident numérique vers l'extérieur.

L'établissement doit préparer par anticipation, des premiers contenus de communication de crise à destination du grand public et de ses organes de tutelle.

Un document ANSSI précise des éléments pour anticiper et gérer sa communication.

2.2 La communication interne

Pour permettre une bonne compréhension de tous, il est nécessaire de diffuser régulièrement des messages d'information à l'ensemble des personnels, pour les rassurer et identifier un calendrier de reprise du fonctionnement normal en cas de fort impact et partager les consignes essentielles en matière de sécurité numérique.

L'indisponibilité du système d'information peut entraîner l'indisponibilité des canaux habituels utilisés pour la communication interne. Des canaux alternatifs pour la communication internes doivent avoir été préalablement prévus. Une communication régulière du personnel de l'établissement nécessite d'être mise en œuvre tout au long du processus de gestion de crise :

- Annonce de la situation de crise ;
- Information régulière sur l'avancement des interventions ;
- Retour à la normale, fin de crise.

2.3 La communication externe

Dès la mise en place du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, il doit exister une concertation étroite entre l'ARS et le directeur de l'établissement pour préparer des éléments de communication afin que ne soient pas délivrées des informations erronées ou contradictoires. En parallèle, les différents acteurs s'engagent à communiquer les éléments aux différents interlocuteurs. Par exemple, l'ARS prendra en charge la communication auprès des établissements de santé voisins de l'établissement touché par une cyberattaque.

Les éléments de langage lors d'une situation de crise numérique nécessitent d'être formalisés en lien avec les organes de tutelle (ministère de la Santé et de la Prévention, ARS).

Une attention particulière doit être portée au respect de la vie privée des personnes et au secret médical.

Il sera nécessaire de prévoir des canaux de communication directs entre la cellule de crise et les organes d'appui (ANSSI, CERT-Santé, CERT-FR et les différents partenaires).

Un établissement de santé touché par une crise de type cyberattaque, peut en fonction de son ampleur, être rapidement confronté à des pressions internes et externes (médias, patients, partenaires) susceptibles d'affecter sa réputation. Il est donc important que la communication soit intégrée au dispositif de gestion de crise pour accompagner les équipes.

Une attention particulière est à porter sur la communication au regard de la sécurisation des données personnelles des patients pris en charge.

La communication doit se synchroniser avec les parties prenantes à la crise (ARS, ANS, ANSSI, prestataire, etc.). L'organisation de crise se fait sous l'égide des organes de tutelle, l'ARS ou le cas échéant la Préfecture.

Si la crise revêt un aspect médiatique et conformément au plan de gestion des tensions hospitalières et des situations de l'établissement, il est recommandé de désigner une personne exclusivement en charge de la préparation de la communication avec les médias.

Des vecteurs de communication devront aussi être proposés vers les opérateurs de soins en lien direct avec l'établissement (établissements santé, établissements sociaux et médico-sociaux, professionnels de santé libéraux, laboratoires d'analyse, transporteurs sanitaires, cabinets de radiologie…). En cas d'indisponibilité des moyens de communication mail, l'ARS peut assurer ce relais de communication.

Il conviendra au préalable que l'établissement identifie avec précision les catégories d'acteurs à informer.

2.4 Un dispositif d'information auprès des patients et des familles

De la même façon, il convient de préparer un dispositif d'information relatif à l'incident numérique auprès des patients et des familles notamment en cas de violation des données de santé. Une attention particulière sera portée au secteur de la pédiatrie et de néonatologie.

Ce dispositif doit être proposé par le référent communication et le représentant des usagers en lien avec les experts techniques et porté par la direction.

La charte informatique peut également informer les collaborateurs de la bonne attitude à adopter en cas d'incident avéré.

2.5 Les moyens alternatifs de communication

Il sera nécessaire d'identifier des solutions de communication alternatives au sein de l'établissement, y compris avec les organisations externes sans utiliser les systèmes de communication habituels, au cas où ceux-ci seraient compromis par la cyberattaque. Pour cela, il pourra être nécessaire de s'orienter vers les solutions de communication alternatives certifiées par l'ANSSI.

3. Le signalement interne d'une anomalie

3.1 Le signalement interne d'une anomalie du système d'information

Il est nécessaire de mettre en place en amont, une organisation interne et des procédures, y compris la nuit et en période de week-end, qui permettent la diffusion, sans délai, d'alertes vers l'équipe technique du service en charge des système d'information de l'établissement, notamment vers le personnel d'astreinte.

Des procédures de signalement et de réponse en cas de détection d'un incident lié à la sécurité de l'information doivent définir les mesures à prendre à la réception d'un appel signalant un tel événement.

Tous les utilisateurs doivent être informés des points d'entrée, des procédures de signalement et de leur obligation de signaler tout événement lié à la sécurité numérique dans les meilleurs délais (charte, sensibilisation).

Les circuits de remontée nécessitent d'être les plus courts possibles et permettre de caractériser une présomption sérieuse de menace sur les outils informatiques utilisés : signaler toute faille de sécurité observée ou soupçonnée.

3.2 Définir des critères d'alertes internes

La détection, au plus tôt, d'un incident numérique est un élément important dans la gestion d'une cyberattaque. Ces évènements sont souvent difficiles à identifier et à caractériser correctement, car ils peuvent être assimilés à des dysfonctionnements habituels ou même passer inaperçus.

Pour permettre de réduire le périmètre de l'attaque, les critères de signalement nécessitent d'être connus de l'ensemble des personnels de l'établissement, ainsi que les procédures à suivre et les contacts à établir en cas d'alerte. Les circuits de remontée nécessitent d'être les plus courts possibles et permettre de caractériser une présomption sérieuse de menace sur les outils numériques utilisés.

Il est donc nécessaire de mettre en place en amont, une organisation interne et des procédures, y compris la nuit et en période de week-end, qui permettent la diffusion, sans délai, d'alertes vers le ou les destinataires concernés (y compris vers le personnel d'astreinte), notamment les services chargés de la cybersécurité. Une attention particulière sera portée aux nouveaux arrivants (intérim…).

4. La procédure de signalement des incidents numériques

4.1 Informer le personnel pour sécuriser le système d'information

Dès que l'incident est confirmé, une action de communication interne rapide sera nécessaire pour confiner et protéger l'ensemble du système d'information sain de l'établissement de santé.

En effet, dans le cadre d'une crise, les mesures de gestion à mettre en œuvre lors des premières minutes sont stratégiques pour assurer la sauvegarde du système d'information.

Conformément au plan de gestion des tensions hospitalières et des situations exceptionnelles de l'établissement, il convient de disposer d'une procédure pour informer l'ensemble des personnels de l'établissement de santé de la marche à suivre et de l'évolution de la situation et notamment de la levée de l'alerte.

Cette procédure doit pouvoir être mise en œuvre en l'absence du système d'information de l'établissement et des moyens de communication d'usage.

4.2 Le cadre réglementaire du signalement d'un incident numérique

Depuis le 1er octobre 2017, les signalements des incidents de sécurité sur les systèmes d'information sont obligatoires. En effet, le décret n° 2016-1214 du 12 septembre 2016 précise que les établissements de santé doivent signaler les incidents graves de sécurité ayant des conséquences potentielles ou avérées sur la sécurité des soins, sur la disponibilité, l'intégrité ou la confidentialité des données de santé ou sur le fonctionnement normal de l'établissement.

La déclaration doit être réalisée via le portail de signalement des événements sanitaires indésirables. Le signalement permet notamment à l'ARS d'anticiper les modalités de continuité des soins au sein de la région.

De plus, le dispositif réglementaire en vigueur impose une obligation de signalement à l'ANS des incidents « significatifs ou graves » de sécurité.

Les établissements de santé désignés OSE ont l'obligation de déclarer les incidents informatiques auprès du CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques). Cette obligation de déclaration au CERT-FR s'ajoute à l'obligation de déclaration auprès du CERT santé (ex-cellule ACSS) de l'Agence du numérique en santé (ANS).

Cette obligation de déclaration doit permettre aux autorités compétentes (ANSSI, CNIL, CERT-Santé) d'éviter la propagation des cyberattaques à d'autres établissements mais aussi d'assister l'établissement dans la qualification, l'analyse et la réponse à l'incident.

Si un incident numérique implique des données personnelles et présente un risque pour les droits et libertés des personnes, l'établissement doit également informer la CNIL dans les 72h.

Ces déclarations permettent aussi de recenser les incidents de sécurité dont les acteurs de santé sont victimes et ainsi pouvoir définir des politiques publiques adaptées.

4.3 Le signalement aux autorités compétentes

- **Signalement auprès du portail conformément à l'article L.1111-8-2 du CSP**
- https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil
- La déclaration au portail déclenche le signalement au CERT

- **Signalement auprès du CERT-FR (ANSSI)**
- Disponible 7j/7, 24h/24, Téléphone au +33 (0)1 71 75 84 68.
- cert-fr.cossi@ssi.gouv.fr

- **Signalement auprès du CERT-SANTE (ANS)**
- Disponible 7j/7, 24h/24 ; Téléphone au +33 (0)9 72 43 91 25
- https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

- **Signalement sur le site de la CNIL**
- En cas de fuite de données personnelles, il faut signaler la cyberattaque à la Commission nationale de l'informatique et des libertés (CNIL) dans les 72h suivant sa constatation, conformément à l'article 33 du règlement général sur la protection des données (RGPD).
- Un formulaire est téléchargeable sur le site Internet de la CNIL.
- https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

- **Signalement auprès du point focal régional (gestion de crise) de l'ARS**
- L'ARS reçoit notification du dépôt du signalement sur le portail des signalements, sur la BAL, et le retransmet en interne au référent des systèmes d'information, au service chargé de la gestion de crise et à la direction métier concernée.

Il pourra être utile d'informer, outre le signalement aux autorités compétentes, l'équipe de sécurité de l'établissement support de GHT et notamment son directeur général.

4.4 Les éléments à recueillir lors du signalement

Dans la mesure du possible, il sera nécessaire de préparer en amont, une trame d'information à recueillir pour accompagner le signalement. Ces éléments d'indication sur la gravité et le périmètre de l'incident permettront aux agences nationales de calibrer le mode de réponse à apporter.

Ainsi, il pourra être communiqué les éléments suivants :

- L'impact sur le fonctionnement des systèmes d'information de l'établissement ;
- L'impact estimé sur la continuité des prises en charge médicale ;
- Les besoins d'appui en ressources techniques spécialisées ;
- Les besoins d'appui pour assurer la continuité des soins ;
- Relais de l'ARS pour informer/communiquer auprès d'autres opérateurs de soins (établissements de santé, établissements médico-sociaux, laboratoires d'analyses, professionnels de santé libéraux, transporteurs sanitaires, cabinets de radiologie…).

Ces différents éléments permettront notamment à l'ARS d'identifier le plus précocement possible s'il y a lieu de mobiliser d'autres établissements et/ou de déclencher une cellule régionale d'appui au pilotage sanitaire.

5. Une veille sur les *scenarii* et vecteurs d'attaque fréquents

5.1 Une veille permanente sur les typologies d'attaque

Il est nécessaire pour les équipes des services chargées de la sécurité du système d'information de l'établissement, d'effectuer une veille permanente sur les modes opératoires liés aux cyberattaques. La bonne compréhension des mesures et des tactiques utilisées permettra de réduire l'impact sur les capacités et fonctionnalités du système d'information.

Il s'agit d'un point important dans la mesure où les actions correctrices à mettre en œuvre sont différentes selon le type de cyberattaque.

De plus, la qualification « cyberattaque » ou malveillante d'une anomalie n'est pas toujours immédiate. Dans certains cas, plus d'une demi-journée a été nécessaire pour qualifier d'attaque cyber un incident technique.

A ce stade, la menace la plus fréquente relève du rançongiciel à base de chiffrement des données avec ou sans exfiltration des données et menace de publication.

5.2 Les vecteurs d'attaque fréquents

L'hameçonnage, ou « *phishing* », est une attaque informatique qui vise à obtenir des données personnelles en misant sur l'usurpation d'identité (vol d'identifiant).

Les hôpitaux connaissent principalement des attaques par *ransomware*, c'est-à-dire des logiciels glissés dans une pièce-jointe qui une fois ouverte, bloque l'accès aux fichiers et crypte tous les documents.

Le code malveillant du rançongiciel a pour but de bloquer l'accès à votre ordinateur ou à des données personnelles. Le rançongiciel se propage dans tout le système d'information et ses différents composants informatiques pour chiffrer un maximum de données et les rendre inexploitables.

Dans les deux cas, cela conduit à l'obtention par l'attaquant d'un accès initial, dont le catalyseur est très souvent la faiblesse structurelle des annuaires de la structure. On peut noter plusieurs étapes avec par exemple l'accès initial, la latéralisation, l'élévation de privilèges, l'exfiltration de données, le chiffrement des données, la suppression des journaux.

Si des compromissions à la suite de campagnes d'hameçonnage restent fréquentes, les compromissions de machines vulnérables accessibles depuis Internet (notamment via des accès RDP trop peu sécurisés) sont devenues les méthodes privilégiées depuis l'année 2019.

Néanmoins, le « *phishing* » n'est pas le seul vecteur d'attaque.

La recherche de faiblesse dans le système d'information de l'établissement est aussi un important vecteur d'attaque.

De la même façon, plusieurs cyberattaques avec un important impact sur des établissements de santé n'ont pas ciblé en premier lieu l'établissement de santé, mais l'un de ses prestataires.

5.3 L'acte de malveillance

L'incident numérique peut aussi être initié par un personnel interne à l'établissement suite à un acte de malveillance par exemple.

CHAPITRE 3 : SE PREPARER AUX ETAPES A SUIVRE

1. La détection et l'identification du périmètre de la cyberattaque

1.1 Détecter et reconnaître une perturbation informatique

Selon le type d'incident et le système affecté, les perturbations informatiques d'un établissement peuvent être repérées à différents points internes et externes.

Les défaillances ou les irrégularités telles que les processus informatiques fortement ralentis ou les données chiffrées peuvent souvent être remarqués par le personnel de l'établissement. La détection rapide d'une cyberattaque permet de limiter les effets sur le système d'information et de réduire l'impact sur le fonctionnement de l'établissement et la prise en charge des patients.

Cependant, les cyberattaques sont souvent difficiles à identifier et à caractériser correctement, car ils peuvent se faire passer pour des dysfonctionnements ou passer inaperçus :

- Trafic réseau inhabituellement élevé ;
- Espace de stockage plein ou significativement consommé ;
- Usage des processeurs inhabituellement élevé ;
- Création de nouveaux comptes utilisateurs ;
- Tentative d'utilisation / utilisation effective de comptes à privilèges (comptes administrateurs, …) ;
- Comptes bloqués, compte utilisateur exploité en l'absence de l'utilisateur sur site ou en télétravail ;
- Fichiers de traces (journaux/logs) effacés ;
- Fichiers de traces anormalement volumineux incluant un nombre inhabituellement important d'événements.

Ainsi, pour répondre efficacement, il sera important de déterminer le type d'attaque pour déterminer la typologie du plan de réponse à mettre en œuvre : tentative d'intrusion, « *phishing* », attaques DDoS, chiffrement rançongiciels, vol de données ou prises de contrôle de comptes/utilisateurs, détections virales.

1.2 La mise en place d'outils de détection efficaces

Des dysfonctionnements informatiques peuvent également être identifiés grâce à des analyses régulières ou continues des processus de sécurité numérique internes à l'établissement. Ces solutions détectent automatiquement les anomalies et bloquent les éventuelles menaces.

En effet, la mise en place d'un système de détection efficace par du monitoring continu permet de contrôler divers éléments relatifs au fonctionnement du système d'information hospitalier comme par exemple l'exploitation des ressources, le débit, le contrôle des flux, l'utilisation de la bande passante.

Ce dispositif améliore la sécurité informatique en mesurant les activités du système et détecte les anomalies, souvent liées à des attaques.

Bien entendu, ces outils de détection d'intrusion ou d'attaque doivent être couplés à la vigilance humaine.

1.3 Vérifier la capacité de détecter les codes malveillants polymorphes

Les travaux de préparation menés nécessitent d'interroger régulièrement l'établissement sur sa capacité de détection au regard des récentes cyberattaques et notamment des codes malveillants « polymorphes ».

En effet, ceux-ci ont la capacité de modifier leur empreinte afin de déjouer les systèmes classiques de sécurité qui reposent essentiellement sur la reconnaissance des signatures.

La particularité d'un tel code réside dans le fait qu'il génère une nouvelle empreinte à chaque réplication le complexifiant et rendant sa détection, sa mise en quarantaine et son élimination difficile pour les solutions anti-virus.

Les dispositifs de détection qui se basent sur la reconnaissance des signatures peuvent uniquement protéger des codes malveillants connus et laissent donc la possibilité à toutes les variantes de codes malveillants polymorphes d'effectuer des intrusions au sein du système d'information.

1.4 Evaluer la pertinence de mettre en œuvre la technologie EDR

Des outils de détection et de réponse (EDR : Endpoint detection response) permettent de répondre aux objectifs de détection d'attaques inconnues, de lancement de correctifs automatiques contre ces menaces et de réalisation d'investigation à distance. La détection s'effectue sur l'analyse comportementale du code malveillant. Ces outils ont la capacité de détecter, d'investiguer et de remédier au défaut.

La technologie de détection et de réponse au niveau des terminaux EDR est une nouvelle technologie qui complète la stratégie « antivirus » déjà mis en œuvre par un établissement.

Cette technologie fait référence à une catégorie d'outils qui surveillent en permanence les informations relatives aux menaces sur les « End-point » c'est-à-dire les postes des utilisateurs, les serveurs…Son objectif est de détecter les menaces qui pèsent sur les équipements informatiques et d'élaborer une réponse rapide au besoin.

Les flux de données issus des postes utilisateurs ou des serveurs sont acheminés - sous un format anonyme - vers un emplacement central, qui est généralement une plateforme EDR.

La solution utilise l'apprentissage de routine pour analyser les flux de données et effectuer une analyse comportementale. Les informations de routine sont utilisées pour établir une base de référence de l'activité normale afin de pouvoir identifier les anomalies qui représentent une activité suspecte. Certaines solutions « EDR » incluent des options qui permettent à partir d'exemples concrets de cyberattaques de comparer l'activité du réseau avec ces exemples pour détecter les attaques.

Toutefois, pour qu'elle soit efficace, cette solution doit être mise en regard des ressources en cybersécurité à mobiliser pour gérer les alertes au sein de l'établissement pour l'administrer et l'exploiter.

Aussi, ce type de solution requiert sa remise à niveau régulière pour prendre en compte les fonctionnalités nouvelles.

1.5 Identifier le périmètre et le chemin de compromission suivi

Une fois qu'une alerte a été reçue concernant un incident, l'étape suivante consiste à obtenir le plus de détails sur le périmètre de l'attaque, le chemin de compromission qui a été suivi pour altérer le fonctionnement du système d'information de l'établissement, les vecteurs potentiels d'infection et les fonctions malveillantes.

Dans le cas d'une cyberattaque, la source initiale de l'attaque doit également être déterminée.

1.6 Collecter les journaux d'incident des éléments de sécurité

D'un point de vue opérationnel, il s'agira de prévoir en amont, une organisation qui permettra à l'équipe chargée de la sécurité du système d'information de recueillir du service identifié comme étant à l'origine de l'intrusion, les journaux d'incident des éléments de sécurité dont les antivirus et les VPN.

La démarche d'investigation doit déterminer la cause, l'ampleur, l'impact de l'attaque et la durée potentielle d'indisponibilité des outils numériques et définir la stratégie de confinement.

Cette opération permettra d'analyser la durée potentielle d'indisponibilité des outils numériques et définir la stratégie de confinement ainsi que les priorisations de remise en fonctionnement des systèmes impactés.

Il s'agit d'une étape essentielle qui permettra aux équipes chargées de la sécurité du système d'information de mettre en place la meilleure stratégie de confinement et de continuité d'activité.

2. Le recensement des systèmes corrompus et la qualification de l'incident

2.1 Identifier les systèmes corrompus

Les réseaux, systèmes ou utilisateurs potentiellement corrompus doivent être identifiés : nombre de postes administrateurs, nombre de postes utilisateurs, nombre de serveurs, type de systèmes touchés.

Ces informations sont importantes pour attribuer un niveau de gravité à l'incident numérique qui détermineront le type de réponse à adopter en regard.

Des exercices réguliers devront être effectués pour déterminer rapidement les systèmes corrompus.

Les récents épisodes ont démontré que cette étape de vérification avait été longue et complexe à effectuer.

2.2 Contrôler l'intégrité des sauvegardes

Il s'agira de s'assurer si les sauvegardes régulières réalisées sont compromises :

- Vérifier que les sauvegardes n'ont pas été chiffrées ;
- Vérifier s'il y a eu une exfiltration de données.

Les modalités de vérification de l'intégrité des sauvegardes nécessitent d'être anticipées.

Des exercices réguliers devront être effectués pour déterminer rapidement la qualité et l'intégrité des sauvegardes. Les récents épisodes ont démontré que cette étape de vérification de la sauvegarde avait été longue et complexe à mettre en œuvre.

Il est recommandé de suspendre toutes les sauvegardes tant que l'origine de l'intrusion n'a pas été identifiée.

2.3 La qualification va déterminer le déclenchement du volet numérique

Afin de déclencher le volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, il est nécessaire de qualifier précisément le type d'incident, son niveau de gravité, les vecteurs potentiels d'infection, les fonctions malveillantes, le périmètre de compromission ainsi que son impact potentiel sur le système d'information.

Il sera nécessaire de définir les critères qui permettront de qualifier l'incident numérique.

Cette qualification est une étape importante car l'impact sur l'offre de soins et la continuité des prises en charge va déterminer le déploiement du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles et le niveau de réponse approprié.

Le maintien de la qualité et de la sécurité des prises en charge devra toujours être la priorité.

Au regard de la cartographie réalisée et notamment des systèmes d'information essentiels à la continuité de fonctionnement de l'établissement décrits dans la partie 1, il sera nécessaire d'évaluer si ces applicatifs sont fonctionnels et dépourvus d'actions malveillantes.

Par exemple, il s'agira dans un premier temps de vérifier si les serveurs utilisés pour consulter les données patient, l'applicatif de prescription des médicaments, l'applicatif des examens de laboratoire et d'imagerie, les applicatifs relatifs au plan de traitement au sein du service de radiothérapie sont compromis.

C'est la compromission des applicatifs essentiels de l'établissement et le risque de perte de chance pour les patients pris en charge qui traduira le déclenchement du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles.

3. Le confinement des zones affectées pour réduire la surface d'attaque

3.1 Le confinement des systèmes corrompus pour endiguer l'attaque

Une fois que la cause de la cyberattaque et les cibles potentiellement compromises sont connues, il est nécessaire de contenir l'incident à un périmètre restreint. La réussite d'une attaque de rancongiciel par exemple dépend de la rapidité à laquelle elle peut se propager à travers le réseau d'un établissement. Une réponse rapide peut considérablement réduire l'impact sur l'établissement de santé et empêcher les fonctions malveillantes de se propager.

En effet, certaines attaques ont une portée tellement large que la direction du système d'information de l'établissement de santé ne peut les gérer avant qu'elles n'entraînent des conséquences irréparables. D'autres incidents sont trop techniques pour être résolus immédiatement par les compétences disponibles localement. Par conséquent, il est nécessaire d'endiguer le plus rapidement possible l'attaque par une stratégie de confinement des systèmes.

La partie essentielle du confinement est la prise de décision. En effet, l'évaluation et les conséquences de mesures immédiates à mettre en œuvre (ex isoler l'établissement de santé du réseau) pour permettre l'opération de confinement nécessitent d'être anticipées.

3.2 Des stratégies de confinement différentes selon le type d'incident

Les stratégies de confinement varient en fonction du type d'incident. Par exemple, la stratégie pour contenir une infection par un code malveillant transmis par e-mail est assez différente de celle d'une attaque DDoS basée sur le réseau.

Il est donc nécessaire de préparer des stratégies de confinement distinctes pour chaque type d'incident majeur, avec des critères clairement documentés pour faciliter la prise de décision.

L'objectif visera à isoler le système d'information de l'établissement pour limiter la propagation du ou des codes malveillants et couper les liens avec les autres établissements de santé.

3.3 Des mesures immédiates pour réduire la surface d'attaque

Au regard de la classification de l'attaque, il pourra être nécessaire de mettre en œuvre des mesures immédiates pour l'endiguer mais celles-ci doivent être anticipées car non dénuées de risques parfois plus lourds que l'incident lui-même.

Il est donc important d'anticiper l'impact de ces mesures au regard de la gravité de l'incident numérique.

Dans certains cas, il sera nécessaire de déconnecter l'ensemble du réseau pour empêcher l'attaquant d'accéder à l'ensemble des ressources du système d'information de l'établissement.

Au regard du niveau de gravité de l'incident numérique, il pourra être nécessaire selon les typologies d'attaque de :

- Déconnecter immédiatement tous les appareils compromis : isoler du réseau et du système de stockage ;
- Éteindre tous les appareils qui n'ont pas été infectés afin de limiter les dommages ;
- Déconnecter les unités de stockage externe ;
- Lancer une analyse antivirale.

En fonction du type d'attaque, il sera nécessaire de couper l'accès à Internet de l'établissement pour empêcher la propagation de l'attaque, du chiffrement des données et/ou de la fuite des données.

Pour aller plus loin, une fiche réflexe ANS : Réagir à un acte de malveillance.

Pour aller plus loin, une fiche réflexe ANS : Agir contre un maliciel.

4. Le fonctionnement du système d'information en mode dégradé

4.1 Des mesures temporaires à mettre en œuvre

Il est nécessaire de mettre en place des solutions temporaires pour impacter le moins possible les services de soins et administratifs de l'établissement de santé. En effet, les mesures d'isolation, de déconnexion et d'endiguement de la menace nécessitent souvent du temps et l'enjeu prioritaire vise à maintenir des prises en charge satisfaisantes des patients sans accès aux outils numériques.

Il s'agira pour chaque activité de soins de préciser les niveaux de service retenus et les durées d'interruption maximales admissibles pour ces différents niveaux de service, ainsi que les ressources et procédures permettant d'atteindre les objectifs, en tenant compte des ressources critiques qui peuvent avoir été perdues, jusqu'à la reprise de la situation normale.

Ces mesures de contournement devront être mises en œuvre dans le cadre d'une utilisation temporaire et selon des modalités sécurisées.

Bien entendu, une communication préalable devra être mise en œuvre pour préciser le cadre d'utilisation de ces outils temporaires et leur bonne compréhension.

4.2 Des infrastructures temporaires

Il s'agira par exemple de disposer d'ordinateurs portables, de dispositifs mobiles d'accès internet découplés du dispositif de l'établissement, de téléphones mobiles et de supports externes pour permettre des échanges d'information sécurisés avec les différents services cliniques.

Il s'agira de disposer de dispositifs (clés 4G/5G) afin de rétablir une connexion Internet auprès de certains services critiques.

Les opérateurs téléphoniques peuvent être sollicités pour prêter/louer des clés 4G/5G afin de rétablir une connexion Internet auprès de certaines services critiques, comme la télésurveillance des équipements biomédicaux.

Des infrastructures de réseaux temporaires isolées (équipement neuf/sain : serveur et ordinateur portable) pourront être reconstruites au sein de certains services de soins critiques pour permettre aux équipes de soins d'assurer la continuité des prises en charge en mode dégradé.

4.3 Une vigilance à la saturation du réseau

La mise en place de réseau temporaire par l'utilisation des dispositifs mobiles d'accès internet (clés 4G) nécessite une vigilance particulière compte tenu de la saturation probable du réseau au regard du nombre d'utilisateur.

Une solution alternative nécessite d'être proposée pour garantir à tous l'accès.

5. L'éradication par la correction des vulnérabilités

5.1 La suppression des codes malveillants

Une fois qu'un incident numérique de type cyberattaque a été contenu, l'éradication peut être nécessaire pour éliminer les composants corrompus, tels que la suppression des codes malveillants, la désactivation des comptes d'utilisateurs piratés, ainsi que l'identification et l'atténuation de toutes les vulnérabilités qui ont été exploitées.

Ce processus vise à réparer les modifications apportées par le code malveillant. Il s'agira notamment de corriger les configurations non sécurisées. Il est important d'identifier tous les systèmes corrompus au sein du système d'information afin qu'ils puissent être corrigés.

L'ensemble des opérations d'éradication nécessitent d'être formalisées et validées par le RSSI avant mise en œuvre. L'équipe en charge de l'éradication doit consigner l'ensemble des mesures mises en œuvre.

Dans certains cas, une action de redéploiement « d'images » vise à réappliquer directement une version saine du système, sur les postes clients et les serveurs. Cette méthode permet de s'assurer que la présence des fonctions malveillantes est supprimée. Pour certains incidents numériques, l'éradication n'est pas nécessaire car elle sera effectuée pendant la restauration des sauvegardes.

5.2 La correction des vulnérabilités

A l'issue de l'étape d'éradication des codes malveillants, il s'agira de corriger la vulnérabilité du système qui a permis l'intrusion. Il sera nécessaire de procéder à l'application de correctifs au vecteur source de l'intrusion, ou de mises à jour logicielles, la reconfiguration des paramètres du réseau, voire le remplacement de systèmes obsolètes ou non pris en charge.

Des nouvelles règles de sécurité pourront alors être proposées. Des actions de modifications des mots de passe des comptes utilisateurs concernés peuvent être nécessaire avec la nécessite d'élever les niveaux d'authentification à l'aide de techniques d'authentification robuste.

Ces corrections sont nécessaires pour éviter que l'attaquant exploite à nouveau le même vecteur d'attaque.

A l'issue de ces opérations, les services informatiques rétablissent le fonctionnement normal des systèmes, confirment que les systèmes fonctionnent normalement voire corrigent les vulnérabilités pour éviter des incidents similaires.

6. La stratégie de sauvegarde pour anticiper l'étape de restauration

6.1 Des sauvegardes déconnectées du système d'information

La solution de sauvegarde doit être conçue pour permettre une reprise après un incident numérique.

Il doit être facile d'identifier et restaurer la version la plus récente des données sauvegardées. Les données doivent être disponibles. Des exercices devront être conduits pour faciliter cette étape centrale.

Des sinistres, pannes, erreurs et malveillances peuvent conduire à la perte de données voire mettre en péril la continuité d'activités essentielles. Il convient donc de définir et mettre en œuvre des modalités permettant de reprendre les activités interrompues ou de restaurer les données perdues dans les meilleurs délais pour les utilisateurs.

Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers et des applications métiers critiques doivent être réalisées.

Certaines sauvegardes, au moins pour les plus critiques (annuaire central, base de données du DPI, configurations des routeurs, etc.), doivent être déconnectées du système d'information pour prévenir leur chiffrement.

L'usage de solutions de stockage à froid (c'est-à-dire « non connecté » au système d'information de l'établissement et idéalement placée à l'extérieur de la structure), permet de protéger les sauvegardes d'une destruction des systèmes et de conserver les données sensibles à la reprise d'activité.

La stratégie de sauvegarde décrira les règles et recommandations à suivre afin de gérer les sauvegardes permettant d'assurer l'ensemble des opérations nécessaires à la préservation des environnements des systèmes d'information hospitaliers.

Dans le cadre de la stratégie de sauvegarde, on distinguera différents types de données à sauvegarder : données, applications métiers, systèmes et éléments d'infrastructure.

6.2 Une attention particulière pour les données et applications critiques

Le principe général est de dupliquer les informations essentielles des applications utilisées en dehors de la base de données de l'application, sous une forme directement imprimable, pour un fonctionnement en mode dégradé. Les éléments à sauvegarder sont principalement :

- Les données : serveurs, postes utilisateur ;
- Application métier bloc opératoire : planning des interventions ;
- Application métier imagerie : planning des examens ;
- Les applications : sauvegarde des applicatifs métiers ;
- Sauvegarde d'un système d'exploitation / reconstruction rapide d'un serveur ;
- Les éléments d'infrastructure : sauvegarde du paramétrage d'éléments d'infrastructures.

Pour aller plus loin, le guide relatif aux règles de sauvegarde des systèmes d'information de santé.

7. La restauration des systèmes d'information corrompus

7.1 L'application du plan de reprise d'activité PRA

Pour effectuer la restauration des applications métiers corrompues, il sera nécessaire de mettre en œuvre les étapes à suivre du PRA du système d'information.

Le PRA du système d'information définit pour chacune de vos applications métiers, dans un contexte métier donné, les étapes à suivre lors du processus de restauration suite à un incident majeur conformément aux préconisations de l'éditeur du logiciel.

Ce PRA devra déterminer quelles sont les données et les logiciels qui devront être restaurés et dans quelles conditions.

7.2 Restaurer les systèmes et données endommagés

Une fois le périmètre de l'attaque identifiée et le processus d'éradication réalisée, il sera nécessaire de restaurer les systèmes ou les données qui ont été endommagés ou perdus pendant l'attaque.

Les récents épisodes de cyberattaques ont nécessité des temps de restauration particulièrement longs.

Cette opération qui s'effectue à partir des sauvegardes saines peut nécessiter des modifications importantes pour permettre de sécuriser les outils et limiter le risque d'une nouvelle compromission.

Ces opérations de restauration qui visent à remettre en production les outils et systèmes corrompus nécessitent du temps et des ressources importantes. Il s'agit d'une étape importante pour permettre de garantir des fonctionnalités sécurisées.

La phase de restauration est une séquence clé de la stratégie de sécurisation d'un système d'information hospitalier dans la mesure où il sera nécessaire de ne pas réintroduire la menace dans le système.

Planifier et concevoir à l'avance la phase de restauration, adaptée aux besoins spécifiques de chaque établissement, peut faciliter la mise en place des mesures de gestion face à une cyberattaque et relancer les systèmes plus rapidement.

Une hiérarchisation doit être décidée et prévue en amont pour permettre la remise en route dans un premier temps des systèmes les plus critiques.

7.3 Des tests de restauration éprouvés et testés

Une phase de test doit être prévue pour vérifier si les applications métiers restaurées après compromission fonctionnent de façon normale. En effet, le risque de réintroduire la menace dans le système d'information pourrait endommager de nouveau le système d'information. Une fois que leur sûreté est confirmée, elles doivent être réintroduites dans l'organisation.

Dans le cas d'une cyberattaque, l'enjeu immédiat est la restitution des données de l'établissement dans les plus brefs délais.

Afin d'y répondre convenablement, il est nécessaire de mettre en place des tests de restauration.

Des exercices de restauration doivent être planifiés et exécutés à minima une fois par an pour vérifier les séquences de restauration des données sauvegardées. Il est nécessaire de préciser que ces tests doivent être réalisés de manière unitaire mais également en chaîne.

7.4 La restauration des applications, un processus qui peut être long

Le processus qui vise à retrouver un fonctionnement normal est un processus long qui peut prendre plusieurs mois, il est donc important d'être préparé pour tenir dans la durée.

8. La reconstruction des systèmes compromis

8.1 La phase de reconstruction

Lorsque des systèmes applicatifs sont compromis, une reconstruction est alors nécessaire.

Plusieurs scenarii d'opération de reconstruction pourront être proposés en fonction de l'ampleur et de la complexité de l'attaque. Cette étape dépend de la menace et de l'étendue de l'attaque. Ces scenarii viseront à garantir la continuité des prises en charge.

8.2 Le choix de reconstruire les applicatifs au sein d'une zone sécurisée

Pour éviter un cheminement identique par un cybercriminel, il peut apparaitre utile de reconstruire les applicatifs utilisés au sein d'une zone sécurisée et isolée des infrastructures attaquées.

Cela nécessite une nouvelle infrastructure et des matériels neufs pour permettre de constituer une bulle saine et ainsi d'être hors d'atteinte d'une nouvelle attaque.

Ce scénario peut s'avérer utile si l'attaquant dissimule une « charge » lors de son intrusion au sein du système d'information qui pourrait se traduire par une nouvelle infection des applicatifs reconstruits. Lorsqu'une zone sécurisée est ainsi créée, la cellule de crise arbitre les applicatifs à réintégrer par ordre de priorité.

9. Arbitrer la sortie de crise

9.1 Définir des critères de sortie de crise

La clôture d'une crise cyber est une étape importante dans le processus de gestion de crise. Elle ne signifie pas que l'établissement de santé est revenu à son fonctionnement optimal mais traduit que les activités essentielles de l'établissement de santé ont repris.

9.2 Arbitrer la suppression du fonctionnement dégradé

Le processus de reconstruction des outils et systèmes et l'étape de sécurisation renforcée du système d'information s'inscrivent dans une étape longue qui peut durer plusieurs mois. Il s'agira notamment d'arbitrer le maintien ou la suppression des solutions de contournement et réévaluer la mobilisation des effectifs en charge des systèmes d'information.

10. Effectuer un retour d'expérience post attaque rapide

10.1 Analyser les forces et les faiblesses

Le retour d'expérience après une cyberattaque fait partie intégrante du processus, car elle permet aux établissements de réduire le risque de futures attaques et de mieux se protéger et protéger les patients pris en charge.

Aussitôt terminée, la crise doit faire l'objet avec tous les intervenants d'une réflexion permettant d'analyser les forces et les faiblesses montrées par le dispositif, le schéma de l'alerte et les modalités de mobilisation des moyens humains et matériels.

10.2 Tirer les enseignements

Il s'agit donc de tirer les enseignements pour prévenir des attaques similaires, les conclusions du retour d'expérience doivent servir d'enseignements. Cela doit également servir à ne pas réitérer les mêmes erreurs.

Sur la base de ces différents retours, le plan de réponse à incident et la stratégie de sécurité globale de l'établissement de santé doivent être adaptés. Il s'agit de s'assurer de mettre en œuvre les meilleures et plus récentes pratiques.

Cela peut impliquer de revoir les rôles et les responsabilités de l'équipe opérationnelle, de mettre à jour le plan de communication et d'intégrer de nouveaux contrôles ou procédures de sécurité.

Par principe de neutralité, il s'agira de s'entourer de personnes qualifiées extérieures à l'établissement pour effectuer le retour d'expérience le plus pertinent.

Un guide méthodologique pour le retour d'expérience sur une situation d'urgence sanitaire ou d'exercice de simulation est disponible sur le site du ministère de la Santé et de la Prévention.

10.3 Une communication à adapter lors des retours d'expérience

Une attention particulière est à porter sur les retours d'expérience « publics » des incidents numériques qui devront s'effectuer en lien et après accord de la cellule « communication » de l'ARS.

Les modalités de réponse mises en œuvre par un établissement de santé lors d'une cyberattaque ne devront pas décrire dans le détail l'ensemble des mesures et moyens mises en œuvre pour détecter, confiner, éradiquer, restaurer ou reconstruire les systèmes corrompus.

Bien entendu, les mesures d'organisation générales nécessitent d'être rendues publiques afin d'en faciliter la diffusion mais les moyens de défense et de sécurisation des composants critiques sont confidentiels.

Des précisions sur la stratégie d'éradication des menaces cyber pourraient faciliter une action de personnes malveillantes.

Fiche réflexe 4 : Les travaux de préparation du volet numérique

- Disposer d'une astreinte 24h/24 sur la sécurité numérique
- Sensibiliser les personnels au risque numérique et numéros d'astreinte
- Adapter un plan de réponse adapté aux différents scenarii
- Disposer d'une documentation rapidement accessible
- Disposer d'une stratégie de réponse mutualisée au sein du GHT
- Réaliser une cartographie de l'offre de soins et des activités à risque
- Mobiliser des moyens, constituer un stock stratégique au niveau GHT/région
- Préparer des modèles à utiliser pour la communication interne et externe
- Anticiper des moyens alternatifs pour communiquer (interne/externe)
- Former les équipes d'intervention informatique aux différents scenarii d'un incident
- Définir des critères d'alertes internes d'un incident numérique pour le personnel
- Définir une procédure pour informer rapidement le personnel
- Définir une procédure pour signaler l'incident aux autorités compétentes
- Savoir reconnaître une perturbation, mettre en place des systèmes de détection efficace
- Évaluer la capacité de l'établissement à mieux détecter les actions malveillantes
- Savoir qualifier l'incident, le périmètre, les vecteurs d'attaque, les systèmes compromis
- Définir une stratégie de sauvegarde, positionner les sauvegardes hors du SI
- Préparer le confinement, mesures immédiates réduire la surface d'attaque
- Préparer la phase d'éradication par la correction des vulnérabilités
- Disposer d'une méthodologie de restauration des systèmes corrompus
- Disposer d'une procédure permettant le report des hospitalisations non critiques
- Mettre en place des infrastructures temporaires pour permettre le mode dégradé
- Conserver les preuves, dépôt de plainte, demande de rançon
- Réaliser régulièrement des exercices de crise et en tirer des enseignements

PARTIE 3 : L'ORGANISATION DES SOINS

CHAPITRE 1 : L'IMPACT SUR L'ORGANISATION DES SOINS

1. Le pilotage de la continuité des soins

1.1 Le pilotage de l'ARS

La réponse sanitaire à mettre en œuvre lors d'un incident numérique majeur et notamment d'une cyberattaque nécessite un pilotage robuste sous l'égide de l'ARS.

Ce pilotage doit prendre en compte toutes les composantes de l'offre de soins (hôpital, ville, médico-social) et permettre des échanges réguliers entre professionnels de santé impliqués dans la prise en charge des patients pour notamment faciliter la coopération et la coordination des acteurs.

Pour assurer ce pilotage, la cellule de crise de l'ARS devra disposer en temps réel, des capacités d'accueil et de prise en charge sur son territoire, en particulier des capacités d'hospitalisation immédiatement mobilisables et disponibles avec un focus sur les services sensibles comme les unités de soins critiques que ce soit pour les adultes ou pour la pédiatrie.

Le SAMU-Centre 15, qui est au cœur du dispositif de régulation des soins hospitaliers et de ville, doit en être informé.

Le dispositif de réponse régionale doit notamment prendre en compte les outils d'organisation des Groupements Hospitaliers de Territoires (GHT).

1.2 Organiser la continuité des soins avec les établissements du territoire

Le fonctionnement en mode dégradé devra aussi prévoir la continuité des prises en charge des patients en lien avec les établissements de santé du territoire.

Des travaux préparatoires devront prévoir l'accueil de ces patients et notamment des professionnels de santé chargés du suivi.

Ces dispositions sont prises par l'ARS dans le cadre du dispositif ORSAN notamment dans la DST « évacuation des ES et ESMS ». L'établissement de santé s'appuie en tant que de besoin sur l'annexe « stratégie de déprogrammation et de reprogrammation des soins » de son PGHTSSE.

1.3 Vérifier la capacité d'admission de nouveaux patients

Au regard de l'impact de l'incident numérique sur l'établissement et de la capacité des services de soins à assurer des prises en charge en mode dégradé, il sera nécessaire de quantifier la capacité de l'établissement à accueillir de nouveaux patients en adoptant une réflexion par filières de soins. L'établissement devra lister par service et spécialité, les motifs de recours à l'hospitalisation qui pourraient être différés sans préjudice pour le patient.

Ainsi, il sera nécessaire de définir les limites des capacités (ressources humaines, lits…) afin d'identifier des seuils à partir desquels il sera nécessaire de faire appel à d'autres sites hospitaliers.

1.4 Choisir de transférer certains patients vers d'autres établissements

Les transferts de patients représentent toujours une situation à risque. C'est pourquoi ils doivent se faire de manière ordonnée sous pilotage de la cellule régionale d'appui au pilotage sanitaire (CRAPS) de l'ARS.

Un premier recensement des patients permettra d'identifier ceux dont l'état clinique est compatible avec un transport sans risque de dégradation clinique. L'organisation des transferts s'effectue sous la coordination de l'agence régionale de santé.

Si cette solution est à envisager, la considérer comme la solution à mettre en œuvre pour faire face à une cyberattaque nécessite une analyse robuste.

1.5 Quantifier en continu l'impact sur la qualité et la sécurité des soins

La stratégie de mise en œuvre d'un fonctionnement en mode dégradé doit aussi permettre de quantifier l'impact sur la qualité et la sécurité des soins et vérifier en continu que les soins prodigués sont appropriés aux patients pris en charge.

Les conséquences de la dégradation du fonctionnement des systèmes d'information sur l'offre de soins (continuité des soins et capacité d'accueil de nouveaux patients) est prise en compte dans le plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles qui peut être activé au niveau du plan de mobilisation interne voire du plan blanc en cas de perturbation majeure.

La mise en œuvre des dispositions du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles dans le cadre d'un pilotage assuré par la cellule de crise hospitalière doit être conjointe de celles prévues dans le volet numérique. Cette évaluation permettra de disposer en continu d'éléments permettant de décider à quel moment réorienter certains patients vers un autre établissement.

Dans le cadre du dispositif ORSAN sous pilotage de l'ARS, il peut être nécessaire de prendre toutes les mesures nécessaires en lien avec le SAMU pour organiser le transfert de certains patients critiques au plus tôt vers un établissement qui sera en mesure de le recevoir et de lui fournir les soins rendus nécessaires par son état de santé.

2. L'organisation des soins en mode dégradé

2.1 Le réseau téléphonique et la messagerie

De la même façon, le réseau téléphonique et la messagerie de l'établissement de santé peuvent être rendus inaccessibles.

Il est nécessaire de prévoir des modalités de fonctionnement dégradé et notamment de formaliser un plan de continuité d'activité.

2.2 La gestion du poste de travail : déconnecter et éteindre son ordinateur

Il est nécessaire de rappeler à l'ensemble des professionnels de santé et plus généralement aux personnels de l'établissement d'éteindre leurs ordinateurs lorsqu'ils quittent leur poste de travail. Laisser son ordinateur en veille et connecté à Internet augmente le risque d'être la cible d'une intrusion.

Des réflexes simples à adopter permettent de réduire cette probabilité : lorsqu'un utilisateur doit s'absenter, il peut fermer sa session. En fin d'utilisation, il est conseillé de se déconnecter d'internet et d'éteindre son PC.

Les récentes intrusions (judicieusement positionnées un vendredi soir) ont élargi des périmètres de compromission dans la mesure où de nombreux PC sont restés allumés.

2.3 L'offre de soins

Un incident numérique et notamment une cyberattaque, peut se traduire dans la plupart des cas par l'impossibilité pour le personnel soignant d'accéder aux dossiers des patients, et donc à la liste de leurs traitements ou de leurs antécédents médicaux ; des impossibilités d'effectuer des demandes d'examens d'imagerie ou d'examens de biologie en urgence.

Les logiciels métiers, les systèmes de stockage en imagerie et les applications métiers liées aux admissions des patients peuvent aussi être rendus inaccessibles.

Il est ainsi essentiel d'anticiper ces conséquences et de coordonner les mesures de gestion propres à ce type d'événement sous l'égide de l'ARS, notamment pour la déprogrammation d'actes médicaux et la régulation de l'offre de soins sur le territoire afin d'assurer la continuité de l'accès aux soins des populations.

L'ensemble des services de soins utilisant des échanges de données ou des dispositifs connectés pourraient aussi être concernés par une avarie du système d'information de l'établissement.

L'impact d'un incident numérique sur le fonctionnement d'un établissement de santé peut être immédiat et avoir des répercussions différentes telles que :

- Panne du réseau téléphonique (standard inaccessible) et de la messagerie ;
- Impossibilité de contacter le SAMU-Centre 15 ;
- Planning du bloc opératoire indisponible ; visualisation des images au bloc indisponible ;
- Dossier patient informatisé inaccessible ;
- Gestion du patient perturbée : admissions, étiquettes patients, certificats de décès ;
- Logiciel métier non fonctionnel (imagerie, pharmacie, laboratoire…) ;
- Centrale de monitorage non fonctionnel (moniteur multiparamétrique, ventilateur…) ;
- Panne du réseau GTC (chauffage, climatisation, traitement d'air…) ;
- Demande d'examens d'imagerie, de laboratoire indisponible ;

- Rendu de résultats de biologie, compte rendu d'examen, accès à l'historique des examens indisponible ;
- Arrêt des séances de radiothérapie, de chimiothérapie ;
- Disparition des plannings de rendez-vous et plans des lits ;
- Absence de traçabilité à la stérilisation ;
- Etc.

2.4 Les dispositifs médicaux

De nombreux dispositifs médicaux sont connectés au réseau de l'établissement de santé pour permettre des échanges de données, de réaliser des opérations de télésurveillance, de faciliter les opérations de gestion de la maintenance à distance ou pour assurer la surveillance à distance des dispositifs médicaux par la gestion des alarmes.

En effet, une centrale de surveillance permet par l'intermédiaire du réseau de l'établissement ou d'un réseau sans fil, d'assurer la surveillance continue de plusieurs patients : moniteurs multiparamétriques, respirateurs de réanimation, pompes à perfusion, pousse-seringues, pompes à nutrition et les appareils de dialyse.

En cas d'incident numérique, la mise en réseau pourrait être perturbée et cette possibilité de surveiller à distance les patients seraient compromises.

Des recommandations de l'ANSM précisent des éléments à mettre en œuvre : « Cybersécurité des dispositifs médicaux intégrant du logiciel ».

2.5 Les fonctions logistiques

Les fonctions supports telles que la distribution des médicaments, la gestion des repas, la gestion des déchets, la stérilisation, la restauration collective, le transport interne, le service coursier - participent à l'organisation et la continuité des soins d'un établissement de santé.

Il est ainsi nécessaire de s'assurer que l'ensemble des volets logistiques prévoient des modalités de fonctionnement dégradés.

Une vigilance particulière sera portée sur la logistique liée au transport interne qui sera fortement sollicité lors d'un épisode de cyberattaque.

2.6 La gestion centralisée/technique des bâtiments (GTC/GTB)

La gestion centralisée/technique des bâtiments (GTC/GTB) correspond à la gestion de tous les systèmes de contrôle.

La gestion technique des bâtiments pourrait être impactée compte tenu des dispositifs de régulation mis en œuvre : gestion centralisée du traitement d'air des salles à environnement maîtrisé, système de climatisation/ventilation, démarrage des groupes électrogènes, ascenseurs et autres équipements qui sont aujourd'hui présents dans de nombreux bâtiments hospitaliers.

Historiquement ces systèmes de GTC/GTB fonctionnaient de manière isolée avec leurs propres installations de contrôle connectées sur des réseaux dédiés distincts. Désormais, ils sont de plus en plus intégrés et connectés aux systèmes informatiques utilisés pour la gestion et l'administration des établissements de santé.

Il est donc nécessaire de disposer de contre-mesures de fonctionnement en mode dégradé en cas d'indisponibilité de la gestion centralisée des bâtiments hospitaliers.

2.7 La gestion administrative

L'ensemble des fonctions administratives, notamment la gestion du codage des actes, la facturation, la gestion des ressources humaines, le système de paie, pourraient être dégradées sans l'utilisation des applications métiers.

Il s'agira de définir des modalités dégradées pour permettre la continuité de ces fonctions administratives.

3. Les procédures du mode dégradé et les exercices

3.1 Des procédures documentées stockées hors du système d'information

Il est nécessaire d'anticiper la stratégie du fonctionnement en mode dégradé qui sera adoptée pour faire face, par ordre de priorité, aux différentes typologies de cyberattaque selon la gravité de leurs effets et leurs probabilités de survenue.

Il pourra être fait référence aux procédures dégradées existantes dans les applications informatiques, qui permettent d'avoir accès à des documents imprimables (ex : synthèse dossier patient, prescriptions...) sur des postes informatiques sans accès réseau.

Ces modalités de fonctionnement devront préciser les ressources et les niveaux de service minimum indispensables.

Ces mesures de gestion seront nécessairement évolutives, car les modes de prises en charge évoluent au regard notamment des innovations technologiques et des liens numériques avec des entités extérieures.

Un cahier de procédures opérationnelles imprimé en plusieurs exemplaires doit être mis à disposition des différents services concernés.

3.2 Des procédures connues et testées grâce à des exercices réguliers

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

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

Enfin, il est important dans la préparation d'un fonctionnement en mode dégradé, de s'assurer que ces procédures dégradées soient connues des professionnels et testées régulièrement - ce point est essentiel - lors d'exercices spécifiques.

3.3 Des exercices réguliers nécessaires

Des exercices réguliers devront être réalisés pour identifier les lacunes du dispositif « mode dégradé ».

3.4 Une agilité des services de soins

Lors d'un incident numérique ou d'une cyberattaque, l'établissement de santé doit pouvoir être prêt à fonctionner en mode dégradé pour assurer la continuité et la sécurité des soins pour chaque patient.

En effet, les étapes relatives à la détection, l'éradication, la restauration et si nécessaire la reconstruction des systèmes d'information corrompus sont des actions qui peuvent prendre du temps.

L'organisation des soins en mode dégradé devra prendre en compte les modalités de prise en charge mais aussi décliner le fonctionnement dégradé des fonctions supports telles que logistiques ou techniques. Des modalités de fonctionnement doivent donc être anticipées pour permettre une agilité d'organisation.

Ces procédures devront être connues de l'ensemble des professionnels de santé, imprimées et stockées au sein des services.

4. Le soutien nécessaire aux équipes

4.1 Veiller au soutien des équipes

En temps de crise, il est nécessaire de faire preuve de réactivité mais aussi de recul pour garantir le bon déroulement des plans de réponse, canaliser les inquiétudes, fournir le juste niveau d'information et mettre en place toutes les mesures de soutien nécessaire aux équipes.

L'organisation du fonctionnement de l'établissement en mode dégradé peut générer du stress au sein des équipes.

Il est nécessaire de prendre en compte les conséquences d'un incident numérique majeur sur les personnels et anticiper des mesures pour réduire l'impact.

Le retour d'expérience des récents incidents numériques au sein des établissements de santé caractérise notamment la nécessité de prendre en compte l'épuisement durable des agents les plus impliqués, confrontés à des horaires de travail et à une pression psychologique importants.

Une pratique du « binômage » associée à une attention renforcée des conditions de travail sont indispensables pour permettre aux équipes techniques et aux professionnels de santé de rester mobilisés.

CHAPITRE 2 : LA PRISE EN CHARGE EN MODE DEGRADE

1. L'identification des activités critiques

1.1 Des modalités d'organisation en fonction des composants affectés

Lors d'un incident numérique, les procédures de fonctionnement en mode dégradé peuvent être différentes en fonction des composants du système d'information affectés. Plusieurs évènements peuvent nécessiter le passage en un tel mode :

- Application métier inaccessible ;
- Messagerie indisponible ;
- Serveur de base de données patient inaccessible ;
- Dossier patient informatisé inaccessible.

Il sera nécessaire de mettre en œuvre un fonctionnement en mode dégradé en fonction de la nature et de la gravité de l'incident numérique.

1.2 L'identification des services de soins critiques

Il sera nécessaire d'identifier la liste des activités de soins critiques (urgence, réanimation, bloc opératoire, laboratoire, imagerie, pharmacie…), les processus logistiques clés (approvisionnement, gestion des RH dont le service de paie…) impactés et les modalités de fonctionnement dégradé.

Ces modalités de fonctionnement devront préciser les niveaux de service minimum indispensable.

Les activités de soins supposent l'existence de flux d'approvisionnement extérieurs dont les plus utiles doivent être utilement cartographiés et décrits pour garantir le bon fonctionnement de l'organisation dans un mode dégradé.

2. La prise en charge des patients en mode dégradé

2.1 Le dossier patient informatisé

Il est nécessaire de mettre en place en lien avec l'éditeur de logiciel une procédure dégradée afin de pouvoir accéder, grâce à une sauvegarde (fréquence prédéfinie) des données du DPI, en complète indépendance du système informatique, à l'ensemble des données nécessaires à la réalisation des soins et à la continuité du travail des équipes assurant la prise en charge du patient.

Une solution dégradée sur la base d'un ordinateur couplé à une imprimante locale doit pouvoir être mise en œuvre.

Cette solution permet l'édition des prescriptions et du plan de soins notamment. Ainsi, les données du dossier patient informatisé sont enregistrées à une fréquence choisie et copiées sur l'ordinateur de secours de façon sécurisée.

2.2 Le PC de sauvegarde

En cas d'indisponibilité du système d'information, les données seront immédiatement accessibles aux professionnels de santé et directement imprimées si nécessaire sur l'ordinateur dit « PC de sauvegarde ».

Le PC de sauvegarde :

- Doit fonctionner sur la chaîne de distribution électrique de secours de l'établissement ;
- Doit être un poste de travail dédié à la procédure dégradée ;
- Doit être connecté à une imprimante de façon directe (hors du réseau établissement) et disposer d'un toner de rechange ;
- Doit disposer d'une procédure synthétique décrivant les modalités d'édition du dossier papier ;
- Doit disposer d'un accès sécurisé ;
- Doit disposer d'une fréquence et de modalités de sauvegarde sur un disque dur.

Il sera nécessaire d'identifier la localisation du « PC de sauvegarde » et son éventuelle mutualisation au sein des services afin de permettre une consultation facilitée à tous.

2.3 Le SAS et le SAMU-Centre 15

Les fonctions essentielles des SAMU-Centre 15 sont la régulation des appels médicaux d'urgence et l'envoi de moyens de secours et de soins d'urgence. L'outil informatique est incontournable pour l'activité de régulation médicale et tous les SAMU-Centre 15 sont, à ce jour, informatisés.

En cas d'incident numérique ou de cyberattaque, les SAMU-Centre 15 seront sollicités dans leur fonction de régulation à double titre, pour réguler la situation ayant une incidence sur l'organisation des soins, et pour organiser la continuité de l'activité de régulation elle-même. En effet, dans un dispositif de crise numérique, il s'agira pour la régulation d'accompagner la réorganisation de l'offre de soins au niveau du territoire.

De plus, les services d'accès aux soins (SAS) et les SAMU-Centre 15 constitueront une cible privilégiée en raison de leur action centrale dans le dispositif de régulation.

S'agissant de la situation d'incident numérique modifiant l'organisation des soins, les SAMU-Centre 15 auront un rôle important de conseil médical auprès de la population, nécessitant un message clair quant aux réponses à apporter.

De plus, un plan de continuité d'activité devra prévoir la coordination entre les SAMU-Centre 15, l'interaction avec l'ARS et l'articulation avec les Services d'incendies et de secours et les transporteurs sanitaires.

Il est recommandé en cas d'incident numérique majeur et notamment d'une cyberattaque d'évaluer la nécessité de délester tout ou partie du flux téléphonique entrant par le SAMU-Centre 15 vers les autres établissements de santé du territoire en lien avec l'ARS dans le cadre d'un dispositif d'entraide. Le plan de continuité d'activité doit préciser l'ensemble des procédures métiers et techniques afin de garantir la continuité du service rendu.

Différentes actions seront à mettre en œuvre :

- Informer le SAMU zonal pour permettre une régulation vers d'autres établissements ;
- Activation de la procédure d'entraide en lien avec l'ARS ;
- Mobilisation du SMUR pour procéder à d'éventuels transferts.

Le SAMU-Centre 15 sera en lien avec la CCH par l'intermédiaire du DMC.

2.4 Sécurisation des communications des SAS et SAMU-Centre 15

La sécurisation des SAMU/SAS constitue une priorité face à un incident numérique. Cela nécessite une démarche de décloisonnement et de concertation métier afin de définir les procédures opérationnelles interdépartementales, études des outils techniques et éventuelles mises à niveau nécessaires, conventionnements inter-établissements.

Le dispositif d'entraide opérationnelle doit engager une double réflexion. D'une part dans le cadre d'un projet métier concerté et d'autre part sur le plan technique (ex : la compatibilité des systèmes informatiques, téléphoniques et radio) et juridique afin de sécuriser les appels traités par le SAMU-Centre 15.

Une vérification de la fonctionnalité des interconnections et moyens de suppléance nécessite d'être mise en œuvre pour permettre la sécurisation des appels lorsque ceux-ci sont reroutés ou lors de la mise en place d'une régulation délocalisée prioritairement vers un ou plusieurs autres SAMU-Centre 15, à défaut vers les centres de traitement des appels des services d'incendie et de secours.

Il sera aussi nécessaire de prendre en compte la sécurité des lignes SAMU-Centre 15 avec les différents services de soins (type grande gardes de neurochirurgie, réanimations, centres de polytraumatologie) – ceux-ci doivent bénéficier d'une solution de recours.

2.5 L'accueil aux urgences

L'accueil au sein d'un service d'urgence peut être fortement perturbé dans la mesure où l'identification des patients est un préalable à l'admission.

En l'absence de système d'information, la réorientation des patients vers d'autres établissements de santé en lien avec la régulation du SAMU-Centre 15, peut être envisagée en fonction de l'offre de soins du territoire concerné.

Une orientation vers les structures de ville type « maison médicale » pour les patients qui nécessitent des soins de médecine générale sera privilégiée.

Différentes actions seront à mettre en œuvre :

- Utiliser la procédure dégradée (étiquette) ;
- Récupérer les dossiers « PC de sauvegarde » ;
- Pour les patients sortants, imprimer les documents du dossier.

2.6 Le bloc opératoire

La prise en charge de patients au bloc opératoire peut être complexe sans accès au système d'information. En effet, plusieurs volets de la prise en charge sont informatisés :

- Les données du dossier médical notamment antécédents, consultations d'anesthésie, résultats de biologie et dossier transfusionnel ; la traçabilité du patient, des actes, du matériel et de la maintenance ;
- Le dossier médical per opératoire : surveillance du patient, prescriptions et dispensations effectuées, gestion des consommables, différents comptes rendus de chirurgie, d'anesthésie, de transfusion, du dossier infirmier ;
- L'équipement de vidéotransmission et l'acquisition des images opératoires ;
- La programmation des interventions pour permettre la gestion d'occupation des salles.

Selon l'étendue d'un incident numérique, il est nécessaire de qualifier :

- L'analyse bénéfices/risques des patients pour permettre la déprogrammation d'actes/ interventions ;
- La capacité de transférer les interventions à risque ou complexes vers d'autres établissements ;
- La possibilité de disposer de créneaux d'intervention au sein d'un bloc opératoire mis à disposition par un établissement de santé du territoire pour permettre la continuité des prises en charge dans des conditions de qualité et sécurité ;
- La capacité de l'établissement d'accueil à intégrer les équipes médicales et paramédicales ;
- La nécessité de préserver les capacités du bloc opératoire aux patients dont le pronostic ne permet pas le report sans perte de chance ;
- Le maintien de l'activité de chirurgie conventionnelle hors urgence vitale.

2.7 La stérilisation des dispositifs médicaux

Le processus de stérilisation est une étape indispensable de l'activité du bloc opératoire.

Un incident numérique au sein d'une unité de stérilisation peut avoir des impacts importants dans la mesure où le processus métier est souvent garanti par une application métier dédiée.

Le logiciel métier permet dans certains cas de prioriser le traitement des boites à stériliser en fonction de l'activité opératoire prévue. Le logiciel métier permet de maîtriser l'ensemble du processus ; monitorer les cycles traitement stérile (autoclave, machine à laver…) et décrire la composition des boites et assurer la traçabilité complète des dispositifs médicaux.

Dans le cadre d'un fonctionnement dégradé, il est nécessaire de :

→ <u>Prévoir une sauvegarde régulière :</u>
- Il est nécessaire de prévoir une sauvegarde régulière des données sur un « PC sauvegarde » pour permettre l'édition via une imprimante non connectée au réseau des listes de composition des boites ;
- Ainsi, il pourra être possible de tracer la composition des boites pour permettre l'identification par le service utilisateur (le stérilisateur utilisé, le cycle utilisé, le numéro de lot de la charge réalisée, la date et l'heure de chargement…) ;
- Prévoir malle de secours : procédures, disque dur.

→ <u>Mettre en œuvre une traçabilité manuelle :</u>
- Afin d'assurer la sécurité et la traçabilité, le logiciel métier permet de relier l'ensemble des dispositifs médicaux traités par les systèmes de lavage au patient pris en charge. Il sera donc nécessaire dans le cadre de la procédure dégradée de mettre en œuvre une procédure de traçabilité manuelle ;
- Disposer de formulaire papier pour effectuer le processus de traçabilité ;
- Traçabilité manuscrite des opérations effectuées ; formulaire de réception.

→ <u>Etape de mise en laveur ou autoclave :</u>
- Formulaire de mise en laveur ;
- Identification du numéro de cycle (les données des autoclaves/machines peuvent être récupérées via USB).

→ <u>Etape de recomposition :</u>
- Recomposition des boites à partir des listes de recomposition « papier » ;
- Date de recomposition, date de péremption, nom du dispositif médical ;
- Impression des listes de recomposition.

→ <u>Expédition des boites selon recomposition / validation du listing :</u>
- Impression d'étiquette d'identification des boites ;
- Code de la boite recomposée, nom du service de soins, numéro de circulation ;
- Identifier les DM sur les bons de livraison ;
- Identification de l'opérateur, date de recomposition, date de péremption.

→ Logistique du mode dégradé :

- Disposer de photocopieurs, imprimantes et ordinateurs hors réseau hospitalier pour permettre l'utilisation de matériels et/ou application en mode autonome.

→ Evaluer la possibilité de sous-traiter de façon temporaire l'activité :

- Il est aussi nécessaire d'évaluer la possibilité de sous-traiter temporairement l'activité vers un établissement tiers en identifiant au préalable un « kit de dispositifs médicaux » nécessaires aux chirurgies urgentes, dont le report entraine un risque pour les patients, et définir au préalable son mode de transport ;
- Dans ce cas, les modalités de traçabilité devront être prévues (format papier).

2.8 Les soins critiques : réanimation, soins intensifs, soins continus

La prise en charge des patients dans les unités de soins intensifs, de réanimation ou de soins continus génère une quantité importante des données numériques compte tenu de la charge en soins à mettre en œuvre.

En effet, l'outil numérique permet de garantir l'exhaustivité du recueil des informations médicales, et notamment la traçabilité de la prescription.

L'impact d'un incident numérique au sein des services de soins critiques se traduit par l'indisponibilité d'accès au dossier patient informatisé et au logiciel métier.

De plus, la capacité d'un monitorage centralisé des paramètres physiologiques des patients pris en charge au sein des unités peut être compromise si le réseau informatique de l'établissement de santé est affecté. En effet, le monitorage centralisé permet de collecter en continu les données « patient » des équipements : moniteurs, respirateurs, pompes à perfusion, analyseurs des gaz du sang, pompe à CEC.

Il s'agira donc de mettre en œuvre une organisation dégradée pour permettre une supervision des alarmes des dispositifs médicaux utilisés en cas d'indisponibilité du réseau de l'établissement et notamment de s'assurer que l'application métier dispose d'une procédure dégradée qui permette une continuité de fonctionnement en mode déconnecté de la base de données patients.

Un plan de sauvegarde devra déterminer la fréquence adaptée de recueil des données de l'application métier (plan de soins, dossier patient…) pour permettre en cas d'avarie une restauration rapide.

La pertinence de mise en place d'un dispositif de PC de sauvegarde devra de la même façon être évaluée.

Les réanimations sont aussi des centres névralgiques de communication : appels des SAMU, avis en salle, demande d'intervention en urgence (procédure arrêt cardiaque intra hospitalier), liens avec le bloc, l'imagerie, la biologie, la pharmacie. Une vigilance particulière est donc à apporter à la continuité des communications (lignes d'urgence) lors d'un épisode de fonctionnement en mode dégradé.

2.9 L'imagerie médicale

L'imagerie médicale nécessite un accès rapide et sans interruption notamment lorsqu'il est nécessaire de réaliser des examens d'urgence pour fiabiliser un diagnostic.

L'impact d'un incident numérique au sein d'un service d'imagerie médicale peut se traduire par :

- Indisponibilité de la téléphonie ;
- Indisponibilité du système d'information hospitalier (SIH) donc de l'identité des patients ;
- Indisponibilité du RIS (Système d'Information Radiologique) ;
- Indisponibilité de l'outil « téléradiologie » notamment lors des demandes d'avis (grande garde de neurochirurgie par exemple)
- Impossibilité d'accéder au planning des examens d'imagerie ;
- Inaccessibilité du système d'archivage PACS (*Picture Archiving and Communication System*) ;
- Indisponibilité de la dictée vocale ;
- Indisponibilité du système d'envoi des CRI aux cliniciens en intra institution et à l'extérieur (retour aux CR papier obligatoire) ;
- Impossibilité de facturer les examens.

Dans certaines situations, les radiologues n'auront pas la possibilité de disposer des examens déjà réalisés dans la mesure où le système d'archivage PACS sera indisponible avec une impossibilité de faire transiter les images pour visualisation dans d'autres services de soins ou d'autres établissements de santé.

Au niveau du secrétariat, il sera impossible d'accéder aux applications métiers : planning des examens d'imagerie.

→ <u>Moyen de communication</u>
- Prévoir l'utilisation des téléphones portables alternatifs pour communiquer avec les correspondants habituels ;
- Disposer d'annuaires localisés hors du réseau informatique de l'établissement.

→ <u>Une interprétation des examens sur la console d'acquisition</u>
- Dans certains cas, les interprétations d'images (Scanner, IRM…) ne pourront se faire qu'au niveau de la console d'acquisition dans la mesure où les flux d'information par l'intermédiaire du réseau de l'établissement entre la consoles d'acquisition et les consoles de post traitement seront indisponibles ;
- Dans l'impossibilité de faire circuler les images via le réseau pour permettre le post traitement des images au niveau des consoles satellites pour réaliser les post traitements, il sera nécessaire de réaliser les interprétations directement sur les consoles d'acquisition ;
- Si possible, il sera nécessaire de raccorder des consoles de post traitement directement sur les consoles d'acquisition.

→ <u>Privilégier les examens prioritaires pour prendre en compte la cinétique du mode dégradé</u>
- Ce mode d'organisation dégradé se traduira par des prises en charge complexes à mettre en œuvre ;

- Il sera nécessaire, dans certains cas, de privilégier les examens prioritaires ;
- Evaluer la nécessité de communiquer sur l'annulation des examens programmés.

→ Anticiper la construction d'un réseau local temporaire

- Par anticipation et compte tenu de la criticité de l'activité, il est recommandé d'identifier en amont les équipements nécessaires (serveur, PACS, consoles…) pour construire une infrastructure locale afin de permettre la continuité de l'activité. Ce dispositif autonome permettra la poursuite des prises en charge ;
- Bien entendu, au regard du nombre important d'interfaces avec les autres systèmes d'informations de l'établissement, il s'agira de proposer le schéma de fonctionnement en « circuit fermé » le plus adapté.

→ Compte-rendu d'examen

- Evaluer la possibilité d'utiliser les notes vocales des téléphones mobiles professionnels ;
- Prévoir format de compte-rendu papier, prévoir possibilités envoi compte-rendu papier ;
- Prévoir de façon ultime papier préformaté pour compte-rendu, papier carbone et stylo.

→ Sauvegarde des images

- Il doit également être possible de graver des examens sur CD directement à partir des consoles d'acquisition.

→ Impression

- Les imprimantes sont actuellement le plus souvent des imprimantes réseaux centralisées, parfois impactées en cas de panne.

Actions à mettre en œuvre :

- Un plan de continuité d'activité « imagerie médicale » selon les scenarii et équipements affectés ; ce point est capital et l'expérience même en dehors de toute attaque informatique montre que ce plan de continuité est rarement mis à jour au gré des nouveaux équipements ou changements de procédure ; c'est la colonne vertébrale qui doit permettre de parer à un maximum d'éventualités : pannes partielles ou totales, attaques informatiques ;
- Une stratégie de sauvegarde déconnectée du réseau ;
- Mise en place d'un système fiable de traçabilité papier des identités/actes réalisés/CR provisoires ;
- Entrainement du personnel capable de basculer dans une organisation sans informatique grâce au plan de continuité ;
- Evaluation de la construction rapide d'une infrastructure temporaire (PACS local) en fonctionnement dégradé (serveur, lecteurs CD/DVD, compte-rendu papier, communication par SMS pour cas urgents…) ;
- Evaluation en lien avec les établissements de santé du territoire pour prise en charge des patients externes ;
- Interprétation sur les consoles d'acquisition ; (CR papier, communication par SMS pour cas urgents…) ;

- Sollicitation des fabricants pour prêt de console de post traitement compatible avec la configuration de l'établissement.

2.10 Le laboratoire de biologie médicale

La prise en charge des examens de laboratoire pourrait être fortement impactée en cas d'incident numérique et notamment par l'indisponibilité d'accès au logiciel métier. Il est donc nécessaire de prévoir un fonctionnement en mode dégradé en cas de panne d'un ou de plusieurs de ces serveurs critiques ou d'une cyberattaque.

Ce mode de fonctionnement dégradé doit prévoir la continuité de service et notamment la gestion des examens critiques, les demandes d'examens urgentes, et la communication des résultats. Le mode dégradé implique la mise en place d'une organisation adaptée à la typologie de l'incident numérique : panne d'une ou plusieurs connexions, panne serveur de résultats…).

Il s'agit d'un plateau sensible qui nécessite une vigilance particulière avec notamment l'identification des prélèvements par le mode « étiquette ».

Pour rappel, le dispositif d'accréditation des laboratoires de biologie médicale prévoit la nécessité d'élaborer un mode dégradé et des procédures en cas de panne informatique, selon gravité et quelle qu'en soit l'origine (matérielle ou logicielle), afin d'assurer la continuité d'activité.

En cas d'indisponibilité du système d'information, la procédure dégradée nécessite d'être mise en œuvre selon les modalités suivantes :

→ <u>Sécuriser le circuit du prélèvement :</u>
- Assurer la traçabilité ;
- Chaque prélèvement du dossier se verra affecter un numéro à partir des « étiquettes pré-imprimées/panne » préparées en avance avec numéros uniques pour suivre l'ensemble des prélèvements patient de bout en bout ;
- Génération de numéros avec le nombre de caractères habituellement utilisé au sein du laboratoire ;
- Ce numéro est défini au préalable (il n'est en aucun cas susceptible d'entrer en conflit avec un numéro habituellement attribué par le logiciel métier utilisé).

→ <u>Application métier</u>
- Activer le mode manuel du logiciel métier pour la saisie pré-analytique.

→ <u>Garantir la continuité de fonctionnement :</u>
- Modalités de gestion prioritaire des examens urgents ;
- Renfort en personnel pour les tâches les plus chronophages ;
- Evaluer les modalités de recourir aux laboratoires de ville pour renforcer la réponse aux demandes.

→ <u>Communication des résultats :</u>
- Mettre en place une organisation pour diffuser les résultats sous format papier ;
- Le laboratoire garde un listing papier des résultats ;

- Solliciter le service coursier interne à l'établissement (si existant) ;
- Anticiper le circuit de transmission, doublé d'un appel téléphonique aux cliniciens pour les résultats urgents.

→ Reprise de l'activité normale
- Anticiper les modalités de reprise des données (administratives, résultats, autres).

2.11 La pharmacie à usage intérieur PUI

L'ensemble du système d'information de la pharmacie peut être rendu inaccessible. Les difficultés se traduisent notamment par l'absence de visibilité sur les stocks et l'impossibilité d'accéder aux modules commandes. Il est donc difficile d'effectuer l'approvisionnement des services de soins.

La procédure dégradée consiste notamment à reconstituer les dotations régulières des services de soins et mettre en place un dispositif de gestion des commandes basé sur l'antériorité des commandes passées.

Il est recommandé de :

→ Disposer de sauvegardes régulières sur un support déconnecté du réseau
- La liste des fournisseurs : téléphone, courriel du point de commande ;
- La liste des produits : fournisseur, conditionnement, UCD, CIP, référence fournisseur, lieu de stockage ;
- Les dotations de service : produits et quantités des produits fréquemment utilisés ;
- Les numéros de téléphone des unités de soins.

→ Garantir la continuité de fonctionnement :
- Activer le mode manuel du logiciel métier ; prioriser les examens urgents ;
- Renfort en personnel pour les tâches les plus chronophages ;
- Evaluer les modalités de recours aux laboratoires de ville pour renforcer la réponse aux demandes ;

→ Disposer d'une sauvegarde récente des applications métiers
- La liste des prescriptions informatisées (à mettre en place par la DSI avec le LAP).

→ Disposer de formulaires papiers
- Disposer de formulaires papiers de demande pour les unités de soins ;
- Disposer de bons de commandes papier pour les commandes aux fournisseurs pour envoi par mail (scan) ou solution alternative par portail web ;
- Disposer de photocopieurs, imprimantes et ordinateurs hors réseau hospitalier pour permettre l'utilisation de matériels et/ou application en mode autonome.

→ Moyen alternatif de communication

- Idéalement pouvoir disposer d'accès internet de secours pour échanger sur site ou via mail avec des adresses mail de secours hors périmètre de l'établissement ou sur un réseau secondaire totalement isolé du premier.

→ Mode dégradé des applications métiers et suivi d'inventaire/gestion du stock

- Anticiper tous les modes dégradés des différentes applications (LAP, LAD, reconstitution chimio, stérilisation) et des matériels associés (automates de préparation, de dispensation, autoclaves, laveurs, etc.) avec classeurs papiers pour mettre en œuvre ces modes dégradés ;
- Prévoir des listes d'inventaire papier vierge ou pré formatées par zone de stockage, pour faciliter le suivi en physique de l'évolution de stocks.

- Reprise de l'activité normale
- Anticiper les modalités de reprise des données.

2.12 L'actualisation des données recueillies lors du mode dégradé

Durant la période de fonctionnement en mode dégradé des informations ont été produites principalement sur des documents papiers. En effet, de nombreux examens complémentaires, tels que les examens biologiques ou d'imagerie ont été réalisés et sauvegardés sur des supports mobiles.

Une fois le système d'information de nouveau disponible, il est nécessaire de prévoir un mode opératoire pour reprendre les données générées lors du fonctionnement en mode dégradé du système d'information pour mettre à jour les applications.

Il faut donc conserver les documents utilisés et définir quelles sont les données à reprendre.

Fiche réflexe 5 : organisation des soins en cas d'incident numérique

- Anticiper les modalités de fonctionnement en fonction de la nature de l'incident
- Prévoir une communication adaptée pour les patients / validée par la cellule de crise
- Imprimer les procédures du mode dégradé - informer les personnels
- Préparer un plan de continuité d'activité des fonctions logistiques : déchets, transport…
- Mettre en œuvre un mode dégradé pour les gestions GTC/GTB
- Anticiper l'indisponibilité de la gestion administrative et notamment de la gestion paie
- Réaliser des exercices réguliers du mode dégradé au sein des services critiques
- Prévoir la continuité d'activité de soins avec les établissements de santé du territoire
- Anticiper l'organisation à mettre en œuvre pour le transfert des patients
- Quantifier en continu l'impact du mode dégradé sur la qualité et la sécurité
- Vérifier la capacité d'admission de nouveaux patients en fonctionnement dégradé
- Anticiper les modalités d'accès au DPI en mode dégradé au sein des services de soins
- SAMU-centre 15 : Sécuriser la téléphonie, informer le SAMU Zonal, délestage à organiser
- Accueil Urgence : Prévoir modalités d'accès au DPI, enregistrement manuel, délestage
- Bloc opératoire : Préserver l'activité du bloc aux urgences vitales, délestage
- Transport : Evaluer la possibilité de mettre en place un service coursier interne
- Téléphonie : Prévoir des modalités de communication alternatives
- Communication « type groupe » rapide : Prévoir en amont une application sécurisée
- Stérilisation : Anticiper la sauvegarde, traçabilité manuelle, sous-traiter l'activité
- Monitorage centralisée : Anticiper une modalité de gestion des alarmes centralisée
- Soins critiques : mode dégradé DPI, prévoir l'accès au mode dégradé du logiciel métier
- Imagerie : Privilégier les examens prioritaires, interprétation sur console d'acquisition
- Anticiper la construction d'un réseau local temporaire au sein des services critiques
- Laboratoire : Privilégier les examens prioritaires
- Pharmacie : Privilégier les examens prioritaires

RÉDACTION ET REMERCIEMENTS

Coordination de la rédaction

Aurélie AVONDO-RAY, Conseiller médical pour les crises sanitaires, DGOS

Bast BIDAR, Chargé de mission pour la gestion des risques techniques associés aux soins, DGOS

Sandrine BILLET, Sous-directrice de la performance des acteurs de l'offre de soins, DGOS

Emmanuel COHN, Adjointe à la sous-directrice de la performance des acteurs de l'offre de soins, DGOS

Enzo DELVECCHIO, Chargé de préparation aux situations sanitaires exceptionnelles, DGS

Vamara FOFANA, Chargé de mission Planification, exercice et capitalisation de crise, DGS

Agnès LAFOREST-BRUNEAUX, Chef de bureau accès produits de santé et sécurité des soins, DGOS

Caroline LE GLOAN, Cheffe de bureau systèmes d'information des acteurs de l'offre de soins, DGOS

Clarisse PHILIPOT, Chargée de mission coordination des travaux transversaux, DGOS

Jean-Marc PHILIPPE, Conseiller médical auprès du Directeur général de la santé, DGS

Nicolas VOSS, Adjoint à la cheffe du bureau systèmes d'information acteurs de l'offre de soins, DGOS

Ont également apporté leur précieuse collaboration à l'élaboration de ce guide

Guillaume BAILLEUX DE MARISY, Haut fonctionnaire adjoint de défense et de sécurité, SHFDS

Thomas BAUGNON, Anesthésiste, réanimation pédiatrique, APHP

Anne-Briac BILI, Directrice de cabinet, ARS Bretagne

Stéphane BOUCHUT, Directeur du Système d'Information du GHT Atlantique 17, FHF

Adrien BOURDON, RSSI, GHT 85

Louis BOYER, Président du Conseil National Professionnel de Radiologie G4, CHRU Clermont Ferrand

Damien BRUEL, Chargé de mission au bureau accès aux produits de santé et sécurité des soins, DGOS

Jean Christophe CALVO, Chef département territorial transformation Numérique, CHRU Nancy, FHF

Cécile CANESSE, Cheffe de cabinet, ARS Hauts-de-France

Jean-Christophe CANLER, Directeur général adjoint, ARS Hauts-de-France

Jean-François CHATEIL, Professeur des Universités, Radiologue, CHRU Bordeaux

Jean-Sylvain CHAVANNE, RSSI, CHRU Brest/GHT Bretagne, FHF

Cécile CHEVANCE, Responsable pôle offres, FHF

Nicolas COSTE, Pharmacien hospitalier, APHM

Rudy CHOUVEL, Responsable adjoint du pôle offres, FHF

Jean-Nicolas DACHER, Professeur des Universités - Praticien Hospitalier, Radiologue, CHRU Rouen

Hélène DELAVEAU, Responsable Département Innovation en santé, ARS Bretagne

Henri DELELIS-FANIEN, Directeur médical, SAMU 86, CHRU Poitiers

Laure DUHESME, Cheffe du bureau Santé et Société - Division Coordination Sectorielle, ANSSI

Pascal DURAND, Directeur adjoint, ARS Occitanie

Alain ESPINOUX, Agence du Numérique en Santé, ANS

Jérôme EUVRARD, Directeur du Système d'Information DSI, CHRU Montpellier, FHF

Céline FIASSON, Chargée de mission système d'information en santé, Cybersécurité, ARS Occitanie

Sylvain FRANCOIS, Directeur du Système d'Information DSI, CHRU Rouen, FHF

Isabelle GELEBART, Directrice adjointe Veille et Sécurité Sanitaires, ARS Bretagne

Isabelle GENDRE, Directrice des Systèmes d'Information du Territoire GHT 21, CHRU Dijon, FHF

Hugo GILARDI, Directeur général, ARS Hauts-de-France

Antoine GROS, Praticien hospitalier, Réanimation médico-chirurgicale, CH Versailles

Marie-Christine LABES, Responsable pôle e-santé et transformation numérique, ARS Occitanie

Jacques LABIDURIE, RSSI, CHRU Limoges

Jean-Baptiste LAPEYRIE, Directeur de projets/CTO, Délégation du Numérique en Santé, DNS

Gilles LARROCHE, Chef de projet, GCS e-Santé Bretagne, ARS Bretagne

Romain LEMOINE, Directeur du GCS e-Santé Bretagne, ARS Bretagne

Anne LESQUELEN, Adjointe cheffe de bureau, accès produits de santé et sécurité des soins, DGOS

Stéphane LUCEAU, Responsable du Service Zonal de Défense et de Sécurité, ARS Hauts-de-France

Guy MARTY, Chargé de mission système d'informations de santé et médico-social, ARS Occitanie

Walid MOKNI, Chargé de mission Veille et sécurité sanitaire, DGS

Maxime MOULIN, Directeur de cabinet, ARS Hauts-de-France

Elise NOGUERA, Directrice générale, ARS Bretagne

Jean François PARGUET, Fonctionnaire de sécurité des systèmes d'information, FSSI, SHFDS

Yann PENVERNE, Praticien Hospitalier, SAMU 44, CHRU de Nantes

Stéphane PIERREFITTE, Directeur des innovations technologiques / SI, GHU Paris, FHF

Louise PIHOUEE, Adjointe cheffe de bureau Premier recours, DGOS

Eric POLLET, Directeur sécurité sanitaire et santé environnementale, ARS Hauts-de-France

Mathieu RAUX, Professeur des Universités, Praticien Hospitalier en anesthésie-réanimation, APHP

Pierre SAVARY, Chef du bureau Premier recours, DGOS

Emmanuel SOHIER, Responsable du CERT Santé, Agence du Numérique en Santé, ANS

Bertrand SOMMIER, Secrétaire Général, FHP

Pierre-Olivier TYRAN, Chargé de mission système d'information de Santé, ARS Hauts-de-France

Anne VITOUX, Cheffe de la Mission Qualité et Pertinence, DGOS