|  |
| --- |
| CHU Ynov |
| Analyse Des Risques De Cybersécurité |
| [Sous-titre du document] |

|  |
| --- |
| Xavier Martin  25/04/2025 |

Sommaire

[1. Cadre de l’étude 2](#_Toc202359629)

[2. Sources de risque 3](#_Toc202359630)

[3. Événements redoutés 4](#_Toc202359631)

[4. Scénarios de menace 6](#_Toc202359632)

[5. Mesures de sécurité existantes et vulnérabilités 7](#_Toc202359633)

[6. Gravité et vraisemblance des risques 9](#_Toc202359634)

[7. Plan de traitement du risque et recommandations 11](#_Toc202359635)

# 1. Cadre de l’étude

Cette étude EBIOS® Risk Manager vise à maîtriser les risques numériques du SI du CHU La Timone, en assurant la continuité des soins, la confidentialité des données de santé et la conformité aux obligations (PGSSI-S, RGPD, HDS).

Le périmètre couvre l’ensemble des systèmes cliniques (DPI, LIMS, RIS/PACS), l’infrastructure réseau, les bases de données, les services administratifs, ainsi que les accès internes (postes, Wi-Fi) et externes (VPN, cloud) et les partenaires (fournisseurs de services, prestataires, GHT).

Ce périmètre inclut les équipements biomédicaux connectés et les sites de secours. Les enjeux « valeurs métier » principaux sont la continuité des soins, la confidentialité/intégrité des données de santé (secret médical, RGPD) et l’image de l’hôpital.

Le contexte hospitalier impose des contraintes fortes (SLA très élevés, disponibilité permanente, impératif médical).

La démarche EBIOS RM comprend cinq ateliers : cadrage et socle de sécurité, identification des sources de risque (SR) et de leurs objectifs (OV), scénarios stratégiques, scénarios opérationnels, puis traitement du risque (PCA/PRA et mesures).

Le cadre réglementaire impose notamment la PGSSI-S (sécurité des SI de santé), le RGPD (protection des données perso. De santé) et, pour tout hébergeur externe, la certification HDS.

En pratique, le CHU gère son SI en interne (pas de HDS requis pour son propre SI), mais doit s’assurer que toute sauvegarde ou service cloud soit HDS.

Les guides PGSSI-S fournissent un référentiel de sécurité et de bonnes pratiques que l’établissement s’engage à suivre.

# 2. Sources de risque

# Les sources de menace sont classées en :

# - Internes malveillantes : utilisateur ou personnel technique mal intentionné (ex. sabotage SI, accès non autorisé).

# - Internes accidentelles : erreur humaine (ex. mauvaise manipulation, suppression de données, téléchargement involontaire de malwares, clé USB infectée) . Par exemple, des comportements à risque d’utilisateurs (applications non autorisées, phishing, clés USB) ont été fréquemment observés dans les incidents de santé.

# - Externes cybercriminelles : attaques ciblées par rançongiciels (extorsion), malwares, APT. Les établissements de santé sont ciblés « de façon opportuniste » par des cybercriminels à but lucratif (rançongiciels, exfiltration de données) .

# - États/pays tiers ou hacktivistes : MOA étatiques ou motivations idéologiques, pouvant saboter ou voler des données sensibles.

# - Accidentelles externes : défaillance matériel (panne de datacenter, sinistre, coupure réseau), défautde maintenance.

# - Partenaires/fournisseurs : un fournisseur de services (cloud, VPN, maintenance) compromis peut contaminer le CHU via la chaîne logistique. Par exemple, la compromission de comptes VPN de prestataires a été fréquemment observée comme vecteur initial.

# Dans le secteur de la santé, une large part des incidents récents résultent d’erreurs humaines (phishing, comptes compromis) .

# Le CERT Santé et le CERT-FR soulignent que 86% des incidents 2022-23 visaient les établissements de santé, dont un tiers lié à des compromissions de messagerie (phishing) 123 4 567 8 859910 111213 91, et qu’un autre tiers était constitué d’événements à fort impact (rançongiciel, exfiltration).

# Ces observations confirment que les sources internes (erreurs ou abus) et externes (cybercriminels) sont toutes pertinentes.

# 3. Événements redoutés

Les événements redoutés décrivent les incidents graves à éviter :

Indisponibilité des services critiques de soins (interruption prolongée du DPI, RIS/PACS, LIMS, réseau interne) entraînant un arrêt des soins d’urgence.

Une attaque majeure par rançongiciel pourrait bloquer l’accès au dossier patient électronique, aux résultats d’imagerie et de laboratoire, mettant en péril le suivi des patients.

Les incidents passés ont montré que la coupure du SI perturbe fortement la réanimation, la pharmacie, la radiologie, etc. et rend le DPI inaccessible.

Fuite ou vol de données de santé (vol de DPI, imagerie, documents administratifs), avec violation du secret médical/RGPD.

Par exemple, l’exfiltration avant chiffrement par un groupe de rançongiciel (ex : 11 Go de données patients volées au CHSF) nuit gravement à la confidentialité.

Altération non-détectée des données cliniques (détournement de résultats de tests, modification de traitements).

Un attaquant ayant compromis le système pourrait falsifier des dossiers patients, conduisant à des erreurs médicales.

Cet événement redouté compromet la confiance dans les données.

Atteinte à l’intégrité des images médicales (RIS/PACS corrompu ou altéré), gênant les diagnostics.

Par ex. une corruption de bases PACS compromettrait le workflow d’imagerie.

Impact financier et réputationnel : extorsion par rançon, coûts de restauration, sanctions RGPD.

Panne majeure/sinistre (incendie, inondation, panne électrique) causant la perte d’accès au SI.

Bien que « accidentelle », elle peut immobiliser l’hôpital et entraîner des conséquences proches d’une attaque informatique (indisponibilité prolongée).

Les événements redoutés peuvent se décliner en termes de perte de disponibilité (soins arrêtés), de confidentialité (données exposées) et d’intégrité (données corrompues). Ils servent de référence pour évaluer la gravité des scénarios.

# 4. Scénarios de menace

# Chaque événement redouté peut survenir via plusieurs scénarios d’attaque typiques. En particulier pour les rançongiciels, on distingue :

# Scénario 1 – Rançongiciel par hameçonnage/spear-phishing : un attaquant externe envoie un e‑mail piégé à du personnel hospitalier ou au DSI.L’ouverture du lien télécharge un malware ou le bulletin d’authentification d’un faux site (compromission de crédentials). L’attaquant se fait passer pour un administrateur ou un client VPN et pénètre le réseau interne. Il élève ensuite ses privilèges (compte administrateur ou service vulnérable) et déploie un rançongiciel sur les serveurs critiques. Celui-ci chiffre le DPI, le RIS/PACS et les bases, paralysant l’hôpital et laissant souvent des sauvegardes chiffrées également . Ce chemin d’attaque (phishing → compte VPN/AD compromis → escalade privilèges → chiffrement) est actuellement le plus fréquent.

# Les analyses du CERT-Santé montrent que les vecteurs initiaux identifiés sont majoritairement des comptes VPN compromis (prestataires ou ex-employés) , suivis d’un chiffrement généralisé des systèmes (ex. LockBit) .

# Scénario 2 – Rançongiciel via fournisseur compromis : un prestataire (par ex. support informatique, cloud) ayant accès au SI est infiltré. L’attaquant profite de cette brèche pour déployer un rançongiciel sur les systèmes du CHU. Par exemple, un attaquant pourrait injecter un malware dans un patch fourni, ou capturer les accès VPN du prestataire et l’étendre au réseau hospitalier. Ce scénario de chaîne logistique est redouté car il contourne certaines protections internes.

# Scénario 3 – Menace interne (malveillante) : un utilisateur légitime mécontent ou espion interne utilise ses droits pour installer un ransomware ou exfiltrer des données. Par exemple, un ancien employé ayant conservé ses accès réseau peut lancer des actions post-départ. Même sans intention malveillante, un administrateur mal formé pourrait provoquer une perte de données (effacement involontaire).

# Scénario 4 – Attaque ciblée sur dispositifs médicaux : exploitation d’une faille dans un appareil connecté (pompe à insuline, scanner IRM) pour se propager au réseau. Par exemple, un malware introduit via un scanner de radiologie non patché pourrait se diffuser vers le serveur RIS/PACS.

# Scénario 5 – Erreur ou sinistre accidentel : un dysfonctionnement logiciel ou une panne matérielle majeure (crash de SAN, incendie dans le datacenter) rend les données inaccessibles.

# Un oubli de rafraîchir des sauvegardes ou une mauvaise configuration réseau peut déclencher une perte de service globale.

# Ces scénarios visent à illustrer les chaînes d’attaque possibles qui mèneraient aux événements redoutés ci-dessus. Ils ont pour sources des menaces externes (cybercriminels, failles tierces) ou internes (erreur, sabotage).

# 5. Mesures de sécurité existantes et vulnérabilités

# Le CHU La Timone dispose de mesures de sécurité classiques adaptées à un grand établissement de santé :

# - Gouvernance et conformité : existence d’un RSSI, d’une politique de sécurité alignée sur la PGSSI-S et le RGPD. L’hôpital possède un DPO pour le RGPD et un référent SSI santé. Le plan d’actions Ségur

# Numérique / CaRE a déjà fait évoluer certains outils critiques (DPI, messagerie sécurisée, identification) vers des versions plus sûres.

# - Architecture réseau : mise en place de DMZ et segmentation logique (VLAN) entre les réseaux critiques (soins, administration, guest Wi-Fi) . Par exemple, les bornes Wi-Fi visiteurs et les terminaux métiers sont isolés. Des VLAN distincts gèrent la segmentation du RIS/PACS et du LIMS. Parcours client VPN sécurisé : accès distant via VPN avec certificat ou MFA.

# - Protection périmétrique : firewalls et équipements de filtrage aux frontières (internet, VPN). Un proxy ou passerelle analyse le trafic entrant. Les accès VPN imposent l’authentification multi-facteurs (MFA) pour l’équipe DSI.

# - Contrôle d’accès : principe du moindre privilège appliqué sur les postes de travail (les utilisateurs ordinaires n’ont pas de droits admin) . Les comptes administrateurs sont limités au nécessaire (stations isolées, non connectées à Internet) . Les annuaires (Active Directory) sont configurés avec des audits réguliers et l’authentification forte.

# - Chiffrement et intégrité : les données sensibles (données patients, backups, mobiles) sont chiffrées au repos et en transit. Les clés USB et disques amovibles sont interdits ou chiffrés.

# - Surveillance et journalisation : le SIEM centralise les logs des équipements (pare-feu, VPN, AD, serveurs médicaux). Des règles de détection (antivirus, IDS/EDR) sont en place et mises à jour.

# - Sauvegardes : existantes quotidiennement sur plusieurs niveaux (sauvegarde locale et externalisée).

# Les procédures prévoient la réplication sur un site de secours. Cependant, les attaques récentes ont montré que les attaquants ciblent et effacent souvent les sauvegardes pour empêcher la restauration, soulignant une vulnérabilité : les sauvegardes doivent être hors ligne et chiffrées.

# - Sensibilisation / formation : campagnes de sensibilisation au phishing sont menées régulièrement auprès du personnel médical et administratif, ainsi que des formations sur la sécurité des dispositifs médicaux.

# Malgré ces mesures, plusieurs vulnérabilités persistent : réseau non suffisamment cloisonné (certains flux critiques traversent encore des segments communs), manques possibles de patch sur des équipements spécialisés (pompes, DVR), absence de PRA/PCA formalisés jusqu’alors, et dépendances fortes vis-à-vis de prestataires externes (avec contrôle HDS à vérifier).

# On note aussi le risque d’erreur humaine lors d’une crise (inertie face à une alerte malware).

# 6. Gravité et vraisemblance des risques

En combinant gravité (impacts sur les valeurs métier) et vraisemblance (probabilité d’occurrence), on obtient la cartographie des risques suivante :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Événement redouté | Scénario principal | Source de risque | Gravité | Vraisemblance |
| Indisponibilité massive des systèmes critiques (DPI, labo, imagerie) | Rançongiciel par phishing > compromis VPN/AD > chiffrement | Cybercriminels externes (Ransomware) | Critique (soins stoppés, risque vital) | Élevée (30 hôpitaux attaqués en 2 ans) |
| Vol ou fuite de données personnelles de santé | Intrusion réseau (VPN ou cloud) > exfiltration DPI/DB | Cybercriminels, malveillance interne | Élevée (violation RGPD, perte confiance) | Moyenne-Élevée (cas fréquents) |
| Altération frauduleuse des données cliniques | Compte administrateur compromis > modification base | Malveillant interne/externe | Critique (sécurité patients) | Moyenne (vulnérabilité modérée) |
| Rupture accidentelle majeure (panne datacenter, sinistre) | Incendie/datacenter hors service | Accident technique/interne | Élevée (arrêt soins) | Faible-Modérée (événement rare) |

La gravité des incidents (impossibilité de soigner, atteinte à l’intégrité des dossiers, fuite massive de données) est jugée critique à élever.

Les établissements attaqués mettent souvent plusieurs mois pour rétablir leur SI.

La vraisemblance des attaques par ransomware est élevée : l’ANSSI a enregistré 30 hospitalisations infectées en 2022-2023 (10% des attaques de rançongiciels).

Les campagnes de phishing ciblées étant récurrentes, les menaces liées aux données patients sont classées probables à très probables. En revanche, un sinistre physique reste peu probable mais d’impact majeur. Les niveaux de risque (critique, élevé, moyen, faible) résultent de cette évaluation combinée.

# 7. Plan de traitement du risque et recommandations

Pour maîtriser ces risques, le CHU doit renforcer les mesures techniques, organisationnelles et humaines :

**Mesures techniques :**

Renforcer le cloisonnement du réseau (micro-segmentation par VLAN ou pare-feu internes), notamment entre les systèmes métier critiques et l’administration.

Mettre en place des DMZ pour isoler les serveurs exposés (web, messagerie).

Contrôler les flux : n’autoriser en firewall que les communications nécessaires.

Bloquer le trafic sortant non essentiel et restreindre les privilèges d’accès réseau.

Authentification renforcée : généraliser la MFA sur tous les accès distants (VPN, consoles d’administration).

S’appuyer sur la recommandation ANSSI R10 : limiter les comptes d’administration au strict nécessaire et les isoler sur des postes non connectés à Internet.

Chiffrement systématique des données sensibles : toutes les données de santé en transit et au repos doivent être protégées par chiffrement aux normes (AES 256 bits ou équivalent). Crypter les sauvegardes et les données sur postes mobiles.

Mise à jour et durcissement : appliquer systématiquement tous les correctifs de sécurité sur les OS, applications métiers et dispositifs médicaux.

Suivre les R12/R13 d’ANSSI : supprimer services inutiles, rendre l’authentification obligatoire en BIOS/UEFI, activer le chiffrement intégral des disques.

Journaux et détection : maintenir à jour le SIEM et les bases de signatures antivirus. Déployer un EDR/IDS pour détecter les comportements suspects (mouvements latéraux, chiffrement de masse).

Les découvertes du CERT montrent que des comportements malveillants sont parfois détectés avant chiffrement.

Sauvegardes hors-ligne : selon ANSSI R18, mettre en place des backups offline des données critiques, chiffrés et testés régulièrement.

Conserver au moins une copie déconnectée et hors-site pour se prémunir d’un rançongiciel ciblant les sauvegardes.

Définir la fréquence de sauvegarde en fonction de la criticité (plusieurs fois par jour pour le DPI, moins pour les données statiques).

Plan de reprise (PCA/PRA) : élaborer un Plan de Continuité d’Activité et de Reprise (PCA/PRA) formalisé couvrant les menaces cyber et accidentelles.

Ce plan doit détailler les procédures d’escalade, de basculement sur site de secours, et les modes dégradés de fonctionnement (ex. reprise manuelle des fiches patients).

Des exercices réguliers doivent valider ce PCA/PRA.

**Mesures organisationnelles :**

Gouvernance de crise : mettre en œuvre un plan de gestion de crise cyber (RACI, cellules de crise, cahier de crise).

Constituer un comité de crise pluridisciplinaire incluant RSSI, directeur médico-technique, communication, DPO, etc.

Mettre à jour le « cahier de crise » avec les contacts clés (CERT-Santé, ANSSI, pompiers, juridiction).

Processus internes : documenter les politiques de sécurité et de contrôle d’accès. Instaurer des revues périodiques de droits sur AD (politique R8/R9 ANSSI) et faire auditer la configuration du SI (PCI DSS, ISO 27001).

Compléter le socle de sécurité selon les référentiels PGSSI-S (contrôle d’accès, plan de gestion de malwares, audits internes).

Contrôles tiers : exiger des partenaires cloud, datacenter ou SSO l’accréditation HDS ou des garanties équivalentes.

Réaliser des audits de sécurité chez les prestataires critiques (maintien de sécurité, patch management).

Plan d’intervention spécialisé : prévoir l’appel au CERT-Santé en cas de crise et l’activation d’équipes d’intervention (firewall, forensique).

Maintenir un accord de support rapide avec les éditeurs de logiciels de santé pour les mises à jour d’urgence.

**Mesures humaines :**

Sensibilisation régulière : renforcer la formation des utilisateurs (personnel soignant et administratif) à la cybersécurité, notamment les campagnes de simulation de phishing. Selon le CERT Santé, une large part des intrusions débute par ce facteur humain.

Mettre l’accent sur les gestes barrières (ne pas ouvrir les liens suspects, vérifier les expéditeurs, crypter les postes).

Exercices de crise : organiser des simulations (table-top et test de PRA) au moins deux fois par an.

Cela vaut pour les scénarios ransomware, mais aussi pour une panne datacenter ou une inondation simulée.

Les retours d’expérience doivent alimenter l’amélioration continue.

Ressources humaines : disposer d’une équipe DSI/SI complète incluant un référent cybersécurité et, si possible, un backup RSSI.

Prévoir une permanence (astreinte) pour le RSSI en cas d’alerte.

Documenter la gestion des connaissances (procédures, inventaire des actifs) pour éviter que la perte d’un acteur critique ne bloque la réponse.

Culture de sécurité : encourager la remontée des incidents, informer les usagers (patients et extérieurs) lors d’incidents majeurs pour limiter les réactions négatives.

Chaque mesure proposée découle des failles identifiées : segmentation (R6) pour limiter la propagation, chiffrement (R7) pour préserver la confidentialité, planification (R17/R18/R19) pour la résilience, etc.

Un suivi itératif permettra d’affiner la cartographie des risques au fil des retours d’expérience et de la maturation du SI.

Cartographie synthétique des risques :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risques identifiés | Gravité (impact) | Vraisemblance | Maîtrise existante | Traitements recommandés |
| Rançongiciel bloquant DPI/RIS (indispo. soins) | Critique (arrêt des soins, RIS) | Élevée (attaques fréquentes) | Système de sauvegarde, firewall, antivirus | MFA sur VPN/AD; segmentation (DMZ/VLAN)  back-up hors-ligne, PCA/PRA |
| Vol de données patients (confidentialité) | Élevée (secret médical, RGPD) | Moyenne (exfiltrations réelles) | Chiffrement des DB, contrats HDS | Renforcer l’authentification forte; journaux SIEM analysés; audits RGPD/HDS |
| Altération des données cliniques (intégrité) | Critique (risques médicaux) | Moyenne | Contrôles accès, RBAC | Limitation des droits admins ;  Authentification renforcée ; contrôle d’intégrité (hash) |
| Panne ou sinistre (accident) | Élevée (retard de soins) | Faible | Site de secours partiel | Doublement alimentation, sites redondants ; procédures manuelles dégradées |
| Autres malwares (DDoS, ICS) | Variable | Variable | IDS/IPS, surveillance réseau | Filtrage DoS; sécuriser IOT/ICS; PRA multi-menaces |

Chacune de ces recommandations sera priorisée selon la criticité et un calendrier de mise en œuvre sera établi.

Une évaluation résiduelle du risque sera réalisée après implémentation, afin de valider l’efficacité des mesures et de décider des actions supplémentaires (transfert de risque via assurance, etc.)