[Date]

Xavier Martin

Chu Ynov

Chiffrement des données sensibles au CHU Ynov

CHU Ynov

Table des matières

[Introduction 2](#_Toc202431170)

[1 : Objectifs de sécurité du chiffrement 3](#_Toc202431171)

[2 : Identification des données sensibles 4](#_Toc202431172)

[3. Sauvegardes : outils utilisés, fréquence et architecture 5](#_Toc202431173)

[4. Hébergement (cloud HDS Microsoft Azure et hybride) 6](#_Toc202431174)

[5. Procédures de restauration des données 7](#_Toc202431175)

[6. Stratégie globale de chiffrement : politique, référentiels, gouvernance 8](#_Toc202431176)

[7. Méthodes de chiffrement retenues 9](#_Toc202431177)

[8. Chiffrement des données 10](#_Toc202431178)

[9. Gestion des clés 13](#_Toc202431179)

[10. Chiffrement des Dossiers Médicaux Électroniques (DME) 14](#_Toc202431180)

[11. Solutions de chiffrement utilisées 15](#_Toc202431181)

[12. Protection dans les applications et bases de données 16](#_Toc202431182)

[13. Sécurisation des sauvegardes (intégrité, chiffrement, journalisation) 17](#_Toc202431183)

[14. Sécurisation des transferts de données (chiffrement bout-en-bout, audit) 18](#_Toc202431184)

[15. Contrôle d’accès et séparation des pouvoirs 19](#_Toc202431185)

[16. Plan de contrôle et d’audit du dispositif de chiffrement 20](#_Toc202431186)

# Introduction

Le CHU Ynov traite quotidiennement des données extrêmement sensibles (informations médicales, administratives et ressources humaines).

Pour répondre aux exigences réglementaires (RGPD, certification HDS, référentiels PGSSI-S) et assurer la confiance des patients, le chiffrement des données est indispensable.

Il constitue un levier majeur pour garantir la confidentialité des informations (seules les personnes autorisées peuvent les lire) tout en contribuant à leur intégrité et à leur authenticité.

Le présent rapport technique détaille les objectifs, les méthodes et les dispositifs de chiffrement mis en place (ou recommandés) au CHU Ynov, couvrant les données au repos, en transit et sur les terminaux, ainsi que leur gouvernance.

Les sections suivantes suivent les normes en vigueur (ANSSI, CNIL, PGSSI-S) et font état des solutions métiers utilisées (Veeam, Rubrik, Atempo Tina, BitLocker, etc.) pour la protection du système d’information hospitalier.

# 1 : Objectifs de sécurité du chiffrement

Le chiffrement répond avant tout au besoin de confidentialité : il transforme les données lisibles en données chiffrées illisibles sans la clé appropriée, protégeant ainsi les informations de santé et personnelles contre tout accès non autorisé.

Par ailleurs, même si le chiffrement vise surtout la confidentialité, il s’inscrit dans une démarche globale de sécurité qui inclut l’intégrité (les mécanismes de hachage et de signature numérique garantissent qu’un fichier n’a pas été altéré) et l’authenticité (identification du signataire).

La politique de sécurité du CHU tire profit du chiffrement pour répondre aux impératifs du RGPD (protection des données à caractère personnel), de la norme HDS et de la PGSSI-S (données de santé).

Enfin, le chiffrement contribue à la continuité de service et à la résistance aux cyberattaques : par exemple, des sauvegardes chiffrées et immuables freinent efficacement les ransomwares et assurent la disponibilité des données critiques.

# 2 : Identification des données sensibles

Au CHU, les données sensibles couvrent principalement :

Données médicales et de santé : dossier patient (diagnostics, prescriptions, compte-rendus, résultats d’examens, imagerie, données génétiques, orientation psychiatrique, etc.).

Ce sont des « données de santé » au sens du Code de la santé publique, soumises à obligation de secret.

Données administratives et d’identification : nom, prénom, date de naissance, numéro de sécurité sociale (NIR/INS), coordonnées, situation sociale, etc. (ces données sont souvent cloisonnées du dossier médical et chiffrées à l’aide de clés distinctes, selon les recommandations de la CNIL.

Données RH et personnel : informations sur le personnel hospitalier (diplômes, salaires, état civil, santé au travail), dans le respect de la réglementation sociale (RGPD, Code du travail).

Données juridiques et financières : dossiers des contentieux, facturation patient (y compris mutuelles), comptabilité, paie, etc.

Ces données à caractère personnel doivent elles aussi être protégées par chiffrement adapté.

Tous ces types de données doivent être classifiés au niveau de sensibilité approprié, selon la charte interne du CHU, et pris en compte par les systèmes de chiffrement et de contrôle d’accès mis en œuvre.

# 3. Sauvegardes : outils utilisés, fréquence et architecture

Le CHU Ynov applique la règle éprouvée 3-2-1 pour les sauvegardes : trois copies des données critiques, sur au moins deux supports différents, dont un hors ligne.

Les principales solutions de sauvegarde déployées sont :

Atempo Tina (solution retenue par de nombreux CHU en France) : elle couvre les besoins de sauvegarde des serveurs, bases de données, NAS et postes de travail.

Tina effectue des sauvegardes incrémentielles quotidiennes en ligne, permettant la restauration rapide d’éléments isolés, et des sauvegardes complètes hebdomadaires pour une reprise après sinistre général.

Elle peut également exporter des copies hors site (« coffre-fort » physique ou cloud) pour assurer un stockage externe conforme au principe 3-2-1.

Rubrik (appliances de sauvegarde et orquestration) : utilisé par exemple au Grand Hôpital Est Francilien pour 150 To de données.

Rubrik intègre des fonctions avancées (immuabilité des sauvegardes, rétention WORM, détection de ransomwares, chiffrement à l’échelle du cluster) et réplique les sauvegardes sur plusieurs sites pour haute disponibilité.

Veeam Backup & Replication : en environnement virtualisé VMware/Hyper-V, Veeam gère les snapshots applicatifs et la réplication de machines virtuelles.

Notamment, Veeam supporte les volumes Windows chiffrés par BitLocker pour sauvegarde et restauration (ce qui permet de maintenir le chiffrement des disques sources et cibles pendant les opérations de backup/restore).

Ces solutions sont orchestrées sur une architecture dédiée (serveurs de sauvegarde isolés en DMZ ou sur réseau administratif), avec une segmentation stricte des flux de sauvegarde et des baies de stockage encryptées.

Chaque volume de sauvegarde est chiffré au repos (voir section 8), et un logger de sauvegarde centralise les actions pour audit.

Les fenêtres de sauvegarde sont planifiées hors heures de production, avec des sauvegardes complètes régulières (hebdomadaires) et des incrémentielles fréquentes (journalières ou continues) pour minimiser la perte de données en cas d’incident.

# 4. Hébergement (cloud HDS Microsoft Azure et hybride)

Depuis 2018, Microsoft Azure France (régions France Central/Paris et France South/Marseille) est certifié Hébergeur de Données de Santé (HDS).

Le CHU Ynov peut donc héberger ses données de santé sur Azure (IaaS/PaaS) en restant en conformité avec la norme HDS et le RGPD.

Azure France Central et France South disposent d’availability zones multiples, garantissant une très haute disponibilité (>99,99 %) et la continuité de service.

L’architecture du CHU peut être hybride : certaines applications et bases de données critiques restent on-premise (pour la latence ou contraintes spécifiques), tandis que les services mutualisés (mail, messagerie sécurisée MSSanté, certaines applications d’e-santé) sont déployés sur Azure HDS.

Azure propose une gestion intégrée des clés (Key Vault) et un chiffrement natif des stockages (Azure Storage Service Encryption, SQL TDE) pour les données hébergées.

Les liaisons entre le CHU et Azure sont sécurisées (VPN ou ExpressRoute privé + chiffrement TLS) et dimensionnées en redondance.

# 5. Procédures de restauration des données

Le CHU dispose d’un Plan de Reprise d’Activité (PRA) complet pour la restauration suite à incident (attaque, sinistre, panne majeure).

Ce plan décrit les responsables et les étapes de restauration pour chaque type de donnée.

Les procédures incluent : vérification de l’intégrité des sauvegardes, déploiement des serveurs de secours (virtuels ou physiques), déchiffrement des sauvegardes si nécessaire, tests de continuité applicative et reprise de l’exploitation.

Les sauvegardes sont testées régulièrement pour s’assurer qu’elles sont exploitables et restaurables.

On prévoit notamment de charger périodiquement une sauvegarde dans un environnement isolé pour valider les processus de déchiffrement et de remise en service.

Les RTO (Recovery Time Objective) et RPO (Recovery Point Objective) sont définis avec les métiers et mis à jour après chaque test de PRA.

# 6. Stratégie globale de chiffrement : politique, référentiels, gouvernance

Le CHU Ynov formalise une politique de sécurité du système d’information (PSSI) où figure expressément le chiffrement comme dispositif majeur de protection.

Cette politique s’aligne sur les référentiels nationaux et internationaux : PGSSI-S (pour le secteur santé), référentiel général de sécurité (RGS) de l’ANSSI et normes ISO 2700x.

Par exemple, pour les bases de données de Dossier Médical Électronique (DME/DPI), il est recommandé d’utiliser des algorithmes et des longueurs de clé conformes au RGS, et de gérer les clés selon les meilleures pratiques ANSSI (stockage séparé, rotation, sauvegardes de clés).

Le RSSI du CHU, en collaboration avec le DSI et la cellule risques, supervise la gouvernance du chiffrement :

* Mise à jour des politiques
* Sensibilisation des équipes IT
* Suivis des audits de sécurité et de conformité (HDS, certification, etc.)

Chaque projet ou matériel neuf doit être évalué pour intégration du chiffrement si des données sensibles sont impliquées.

# 7. Méthodes de chiffrement retenues

Le CHU privilégie des standards reconnus et validés :

AES-256 en mode Authenticated Encryption (GCM) pour le chiffrement symétrique des données (disques, fichiers, bases de données).

ChaCha20-Poly1305 sur les terminaux où AES matériel n’est pas disponible.

TLS 1.3 (ou IPsec/IKEv2 pour les VPN) pour chiffrer les communications réseau sensibles. Les anciens protocoles SSL/TLS obsolètes sont proscrits.

RSA-OAEP ou ECIES pour le chiffrement asymétrique (transmission de clés, échanges sécurisés).

Hachage bcrypt/Argon2 pour le stockage des mots de passe utilisateurs, ces algorithmes résistants aux attaques par bruteforce avec sel protégeant les secrets.

Signatures numériques (RSA-PSS, ECDSA) pour garantir intégrité et non-répudiation des données (ex. certificats applicatifs).

Ces choix respectent les recommandations ANSSI (cf. guides de choix d’algorithmes) et les préconisations CNIL.

Les clés cryptographiques utilisées sont de longueurs appropriées (256 bits pour AES, ≥2048 bits pour RSA).

# 8. Chiffrement des données

**a. Au repos**

Disques et serveurs : les serveurs critiques (bases de données, fichiers patients, virtualisation) utilisent le chiffrement de disque au niveau du système de fichiers.

Par exemple, tous les serveurs Windows sont couverts par BitLocker (chiffrement complet du volume C:, data volumes), et les serveurs Linux par LUKS/dm-crypt ou équivalent. Les baies de stockage SAN/NAS sont configurées en mode chiffré (AES-256) lorsque pris en charge par le fournisseur.

Les sauvegardes et archives sont elles-mêmes chiffrées avant stockage (soit par la solution de sauvegarde, soit par l’usage d’un chiffrement de volume sur la cible).

Conformément aux bonnes pratiques, les sauvegardes les plus critiques sont conservées hors ligne et protégées dans des coffres sécurisés, tout en étant chiffrées au repos au même niveau que les données sources.

Bases de données : les SGBD Oracle et SQL Server utilisent le chiffrement transparent des données (TDE) pour chiffrer automatiquement tablespaces et logs au repos.

Par exemple, sous SQL Server on active le TDE qui chiffre les fichiers de la base avec une clé AES stockée en MASTER, protégeant ainsi les fichiers “hors ligne”.

La clé de la base (DEK) est elle-même protégée par un certificat maître ou par un HSM. Ainsi, même en cas de vol d’un fichier .mdf ou .bak, les données restent inaccessibles sans la clé.

**b. En transit**

Tous les transferts de données entre les sites du CHU (réseau interne, SAN, cloud Azure, interconnexion MSSanté) sont chiffrés.

Les principaux canaux sont : VPN IPsec ou SSL VPN pour l’administration à distance, TLS 1.3 pour tous les accès web (portail patient, API applicatives, messagerie interne), SFTP ou FTPS pour les échanges de fichiers sensibles.

Conformément aux recommandations CNIL, lorsqu’un canal traverse Internet ou un réseau externe, on l’encode systématiquement.

Par exemple, la messagerie médicale utilise la plateforme MSSanté (chiffrement de bout en bout), et le protocole SMTP interne est sécurisé (MTA mutualisés HDS, STARTTLS forcé).

Les flux de télétransmission (ex. échanges avec l’Assurance Maladie via Apicrypt ou l’ASIP Santé) reposent sur des certificats S/MIME.

En tout cas, les versions SSL/TLS dépréciées (SSLv3, TLS 1.0/1.1) sont interdites : seules TLS 1.2+ (idéalement 1.3) sont actives sur les serveurs.

**c. Sur appareils**

Les données hébergées sur les postes de travail et appareils mobiles du personnel sont chiffrées de la même façon : BitLocker (Windows) ou FileVault (macOS) protègent les disques d’ordinateurs fixes et portables.

Les clés USB et disques externes utilisés pour transporter des données sensibles sont eux aussi chiffrés (par BitLocker To Go ou VeraCrypt) et conservés verrouillés en coffre lorsqu’ils ne sont pas utilisés.

Tout smartphone ou tablette professionnel est protégé par chiffrement intégral (Android Enterprise ou iOS en mode sécurisé).

En somme, « recourir à un logiciel de chiffrement pour protéger votre poste de travail, serveur, clé USB, disque dur amovible ou smartphone » est une consigne formelle dans l’enceinte du CHU.

# 9. Gestion des clés

La gestion des clés cryptographiques suit des principes stricts : usage d’un service de gestion des clés (KMS), rotation régulière, traçabilité et séparation des rôles.

Le CHU utilise principalement Azure Key Vault (AKV) comme coffre de clés dans le cloud HDS, avec support HSM (module matériel) pour la génération et la protection des clés maîtresses.

AKV permet de centraliser la création, l’import et l’audit des clés AES/RSA utilisées par les services Azure (stockage, base, VMs) et d’y appliquer une RBAC granulaire.

En local ou pour certains usages (par ex. applications critiques), on déploie des HSM physiques (type Thales ou Gemalto) pour conserver les clés privées sensibles hors du cloud public.

La rotation des clés est définie par politique : par défaut, les clés de chiffrement des données critiques (bases, serveurs, certificats SSL) sont renouvelées au moins tous les 2 ans, ou immédiatement en cas de suspicion de compromission.

Le référentiel recommande en particulier de formaliser un processus de gestion des clés (création, sauvegarde, archivage, suppression).

Ce processus documente la protection des secrets (accès strictement réservé aux administrateurs HSM), la sauvegarde isolée des clés (au cas où un HSM tombe en panne), et le renouvellement automatique des clés compromises.

Les responsabilités sont clairement attribuées : le RSSI et le DPO supervisent la conformité du KMS, tandis que l’équipe de gouvernance des infrastructures (sécurité) exécute les opérations techniques, avec cycles de revue réguliers (audit).

# 10. Chiffrement des Dossiers Médicaux Électroniques (DME)

Le Dossier Médical Électronique du CHU (conforme aux exigences PGSSI-S) fait l’objet de mesures de chiffrement spécifiques.

Conformément aux recommandations en cours de validation par la CNIL/ASIP Santé, toutes les données du DME doivent être chiffrées au repos avec des algorithmes et des paramètres conformes au Référentiel Général de Sécurité (RGS) de l’ANSSI.

En pratique, la base de données du DME est protégée par TDE (voir ci-dessus) et les fichiers cliniques (imagerie, documents) sont stockés chiffrés (par ex. Azure Storage Service Encryption).

De plus, la CNIL exige que les données administratives du dossier patient soient gérées séparément et chiffrées avec des clés distinctes, ce qui assure un cloisonnement cryptographique des informations d’identité.

Un plan de sauvegarde et de restauration du DME est en place (copie journalière chiffrée + copies off-site) pour garantir la reprise en cas d’incident.

Enfin, le DME est accessible aux utilisateurs via des sessions authentifiées (MFA) et chaque accès est tracé (référentiel PGSSI-S) pour audit.

# 11. Solutions de chiffrement utilisées

Les principales solutions logicielles embarquant du chiffrement sur le CHU sont :

* Rubrik : en plus de gérer la sauvegarde, Rubrik chiffre les données de sauvegarde au repos via AES-256 (chiffrement natif sur appliance). Cette solution fournit aussi de l’immutabilité (WORM) pour lutter contre les ransomwares.
* BitLocker : utilisée sur tous les serveurs et PC Windows du CHU pour chiffrer les volumes système et data (AES-128/256) avec intégration TPM. Les clés BitLocker sont stockées dans Active Directory et/ou AKV.
* Atempo Tina : la plateforme de sauvegarde intègre le chiffrement des flux (via SSL ou AES) entre l’agent et le serveur, et peut chiffrer les copies finales en cas d’export vers des emplacements tiers. Le CHU de Rouen, par exemple, a pu restaurer l’intégralité de ses données après une attaque grâce aux sauvegardes Tina chiffrées.
* Chiffrement applicatif : plusieurs applications métiers critiques (gestion des RPU, messagerie HDS, téléphonie IP) utilisent des bibliothèques de chiffrement intégrées (OpenSSL, CryptoAPI) pour protéger les données sensibles au niveau applicatif.

Chaque solution est configurée pour utiliser des clés provenant du KMS du CHU (AKV ou HSM), assurant ainsi un contrôle centralisé.

# 12. Protection dans les applications et bases de données

Pour compléter le chiffrement global, les applications et bases de données intègrent plusieurs couches de protection :

- Chiffrement applicatif : pour les données très sensibles (ex. historique médical détaillé, crédits de carte bancaire du patient) traitées par l’application, on peut chiffrer les champs au niveau applicatif avant stockage (avec une clé maîtrisée par l’application). Cela ajoute une couche de chiffrement supplémentaire, même en base.

Chiffrement natif SQL/Oracle (TDE) : comme vu en section 8, toutes les BD critiques activent le TDE pour chiffrer fichiers et journaux de transaction au repos. Oracle TDE couvre aussi le chiffrement de colonnes et tablespaces sensibles.

Tokenisation : les informations sensibles (numéro de carte vitale, numéro de compte bancaire) utilisées à des fins analytiques peuvent être tokenisées. Chaque valeur réelle est remplacée par un jeton non-sensible stocké dans un référentiel sécurisé, limitant l’exposition en cas de fuite.

Hachage des mots de passe : les mots de passe des comptes utilisateurs ou patients ne sont jamais stockés en clair. Ils sont hachés avec un algorithme robuste (bcrypt ou Argon2) utilisant un sel unique par mot de passe.

Par exemple, sous les annuaires LDAP/AD et les bases applicatives, on applique Argon2id pour résister aux attaques par force brute, conformément aux recommandations CNIL.

Aucun mot de passe n’est conservé en clair dans les logs ou les fichiers de configuration.

Ces protections complémentaires visent à ce que, même si un attaquant contournait une couche (ex. vol d’un backup chiffré ou accès illégitime à un SGBD), les données sensibles demeurent inaccessibles sans les clés appropriées.

# 13. Sécurisation des sauvegardes (intégrité, chiffrement, journalisation)

Les sauvegardes doivent être protégées au même niveau de sécurité que les données actives. Ainsi :

Intégrité : chaque fichier de sauvegarde est accompagné d’une somme de contrôle (hash SHA-256) pour détecter toute corruption.

Des tests périodiques de restauration valident l’intégrité globale des copies.

Chiffrement : les volumes de sauvegarde (sur bande, disque ou objet cloud) sont chiffrés avec AES-256. Le protocole de transfert des sauvegardes (SI et cloud) utilise TLS.

La CNIL recommande explicitement de protéger les sauvegardes par chiffrement et de stocker la copie distante dans un lieu sûr.

Journalisation et audit : toutes les opérations liées aux sauvegardes (création de job, restauration, suppression de point de sauvegarde) sont journalisées.

Les logs de la solution de sauvegarde et les accès au coffre de sauvegardes (physique ou cloud) sont collectés et centralisés dans la plateforme de gestion des journaux (SIEM).

Selon l’ANSSI, « les actions sur l’infrastructure de sauvegarde doivent être journalisées et centralisées » pour déceler toute manipulation anormale.

Des alertes sont paramétrées (intégrité brisée, échec de sauvegarde, accès non autorisé, etc.).

Ces mesures garantissent que les données restaurées sont intègres et complètes, et qu’aucune opération de sauvegarde n’a été compromise à l’insu des responsables.

# 14. Sécurisation des transferts de données (chiffrement bout-en-bout, audit)

Les données échangées avec l’extérieur du CHU (patients, partenaires, autres établissements) sont également chiffrées de bout en bout lorsqu’elles contiennent des informations sensibles :

Les mails et messages sensibles utilisent des certificats S/MIME ou PGP entre correspondants. Par exemple, les transmissions de certificats médicaux ou de résultats aux patients via le portail patient sont chiffrées par TLS 1.3 du navigateur jusqu’au serveur (HTTPS) et stockées chiffrées côté serveur.

Les transferts API/WebService entre systèmes utilisent des canaux TLS (REST/HTTPS) avec authentification forte (token OAuth ou certificat client). Les données sensibles ne circulent jamais en clair sur le réseau.

Les réseaux de capteurs médicaux ou IoT (pompes à perfusion, moniteurs) sont sur VLAN séparés et utilisent du chiffrement WPA3 ou protocoles sécurisés (DTLS) pour les communications critiques.

Les connexions inter-sites (hôpital – cloud) se font par VPN chiffré (IPsec ou SSTP) avec double authentification, garantissant que tout transfert entre le CHU et Azure est protégé de bout en bout.

Par ailleurs, chaque transfert de données sensibles fait l’objet d’un audit : les solutions gateways/MTA et les API gateways loguent systématiquement les accès, et les échanges sont tracés par la DSI.

Les journaux d’accès (logs réseau, connexions VPN, SMTP) sont conservés dans une enclave séparée pour permettre des audits a posteriori en cas d’incident.

# 15. Contrôle d’accès et séparation des pouvoirs

La politique d’accès du CHU repose sur un modèle RBAC (Role-Based Access Control) strict.

Chaque utilisateur se voit attribuer des rôles précis (ex. médecin, infirmier, RH, finance) avec des privilèges minimaux (« least privilege ») définis selon sa fonction.

Par exemple, seuls les pharmaciens ont accès en écriture au module de prescription, et seuls les DSI habilités accèdent aux clés de chiffrement.

Les privilèges administratifs (alteration de config, récupération de clés) sont répartis : un administrateur primaire et un auditeur indépendant.

Aucune personne ne détient les droits combinés sur tout le cycle de clé.

Ce cloisonnement garantit la séparation des pouvoirs (ségrégation des tâches) et limite les risques qu’un même acteur malveillant puisse à la fois consulter des données sensibles et altérer le mécanisme de chiffrement.

Techniquement, chaque service (base de données, clé vault, sauvegarde) est configuré avec des comptes de service dédiés et on utilise le moindre accès réseau possible.

Les accès administratifs aux consoles de chiffrement (AKV, HSM, serveurs de sauvegarde) passent par un VPN spécialisé et MFA.

En résumé, l’accès aux données chiffrées est géré à la fois par chiffrement cryptographique et par contrôle d’accès applicatif (identification des utilisateurs, attribution de droits), assurant une double barrière de protection.

# 16. Plan de contrôle et d’audit du dispositif de chiffrement

Le dispositif de chiffrement fait l’objet d’un plan d’audit et de contrôle régulier. Les points clefs sont :

Revue des clés et certificats : un inventaire centralisé des clés (clients et serveurs) est tenu à jour dans l’outillage KMS. Les certificats expirants sont identifiés avant péremption, et les clés RSA/AES sont validées en conformité avec la politique (longueur, algorithme).

Tests de restauration et de déchiffrement : le CHU organise des exercices (par exemple, un PRA trimestriel) où une instance isolée du système est lancée pour restaurer des données chiffrées, afin de vérifier la procédure de déchiffrement et de gestion de clé.

Audit interne / tiers : des audits de sécurité (chez ANSSI ou prestataire certifié) évaluent la bonne mise en œuvre des mesures (par ex. RGPD, HDS, PGSSI-S). Les procédures de chiffrement (algorithmie, rotation, mise en oeuvre) sont vérifiées. La CNIL et les autorités HDS pouvant également demander des preuves de chiffrement pour contrôler la conformité.

Surveillance en continu : la SIEM collecte les indicateurs clés (tentatives d’accès aux clés, échecs de déchiffrement, anomalies de sauvegarde) pour détecter tout comportement suspect. Les incidents liés à la cryptographie (perte de clé, intrusions sur la KMS) sont traités en priorité maximale.

Ces activités sont documentées dans le plan de gestion des risques et dans la PSSI, garantissant que le chiffrement reste efficace face aux évolutions des menaces et des technologies (migrations post-quantiques, etc.).

# 17. Annexes

Glossaire technique

|  |  |
| --- | --- |
| **Terme** | **Définition** |
| Chiffrement | Transformation des données en clair (plaintext) en données chiffrées (ciphertext) illisibles sans clé. |
| Symétrique / Asymétrique | Chiffrement symétrique utilise une clé secrète partagée (ex. AES), asymétrique utilise une paire de clés publique/privée (ex. RSA, ECC). |
| AES-256 | Algorithme de chiffrement symétrique à clé de 256 bits recommandé pour la protection des données. |
| TLS (Transport Layer Security) | Protocole de sécurisation des communications réseau (HTTPS, VPN) assurant confidentialité et intégrité des données en transit. |
| BitLocker | Fonctionnalité de Microsoft Windows pour chiffrer les volumes de disque (Full Disk Encryption). |
| TDE (Transparent Data Encryption) | Chiffrement transparent des bases de données (SQL/Oracle) au niveau des fichiers de données et journaux, sans modifier l’application. |
| HSM (Hardware Security Module) | Module matériel sécurisé pour générer et stocker des clés cryptographiques de façon inviolable. |
| Key Vault (KMS) | Service de gestion de clés centralisé (ex. Azure Key Vault) pour créer, stocker et administrer les clés cryptographiques. |
| PGSSI-S | Politique Générale de Sécurité des Systèmes d’Information de Santé (référentiel national). |
| HDS (hébergement) | Certification « Hébergeur de Données de Santé » exigée pour héberger légalement des données de santé en France. |
| RBAC | Role-Based Access Control, contrôle d’accès basé sur les rôles : permissions associées à des rôles attribués aux utilisateurs. |
| Salage (salt) | Donnée aléatoire ajoutée aux mots de passe avant hachage (ex. bcrypt, Argon2) pour empêcher les attaques par tables arc-en-ciel. |
| 3-2-1 (sauvegarde) | Stratégie de sauvegarde : 3 copies de données, sur 2 supports différents, dont 1 hors site/offline. |

**Architecture type du système de chiffrement**

Une architecture typique du dispositif de chiffrement au CHU comporte plusieurs couches :

**Réseau d’infrastructure :** segmenté (réseau utilisateur, réseau administratif, DMZ sauvegarde), avec firewalls entre chaque zone.

**Serveurs et services HDS :** bases de données et applications critiques hébergées dans un datacenter HDS ou sur Azure HDS, avec les disques chiffrés (AES). Serveurs d’applications et postes de travail en interne.

**Key Management (KMS) :** Azure Key Vault (multi-régions FR) et clusters HSM locaux accessibles via API REST sécurisée. Un plan de secours de clés est stocké en clé USB dans un coffre-fort du DSI.

**Sauvegarde :** Appliances Rubrik et serveurs Veeam situés dans la DMZ de sauvegarde, avec réplication chiffrée vers site distant (ou Azure Backup Vault HDS). Les bandes/stockage lointain sont hors réseau.

**Accès distant :** concentrateurs VPN/IPsec établis entre le siège et le cloud, forment un tunnel TLS. Les sessions des administrateurs passent par une jumpbox chiffrée.

(Un schéma détaillé d’architecture serait ajouté ici en annexe visuelle.)

**Cartographie simplifiée des flux chiffrés**

**Entrée des données patients :** saisie au poste [HTTPS] → application DME → base SQL (TDE AES) → sauvegarde programmée (chiffrée).

**Flux internes :** console admin [RDP TLS] vers serveurs chiffrés ; transferts de fichiers RH/financier [SFTP] chiffrés.

**Échanges inter-hôpitaux :** emails [MSSanté ou S/MIME], API [HTTPS mutualisé], réplications données [VPN chiffré].

**Sécurité des clés :** administration de AKV via interface web [HTTPS+MFA], sorties de clés maîtrisées par HSM hors-ligne.

Cette cartographie assure que toute donnée sensible est protégée dès sa création jusqu’à son archivage, en passant par tous les points de transit, conformément aux exigences réglementaires et aux bonnes pratiques.