

# Meeting Healthcare Security Standards: From Legal Requirements to Technical Implementation

Ambre Journot  
Université Côte d'Azur - Laboratoire  
I3S-CNRS  
Sophia Antipolis, France  
ambre.journot@etu.univ-cotedazur.fr

Karima Boudaoud  
Université Côte d'Azur - Laboratoire  
I3S-CNRS  
Sophia Antipolis, France  
karima.boudaoud@univ-cotedazur.fr

Christian Delettre  
Deltekzen  
Valbonne, France  
christian.delettre@deltekzen.com

## Abstract

Ensuring security of healthcare data represents a pivotal challenge within the medical field. Healthcare professionals, particularly those who practice independently or in the field of alternative medicine, often encounter challenges in implementing secure data exchange methods. Instead, they rely on unsecured channels such as standard email or instant messaging platforms. This practice exposes sensitive patient information to significant risks, including data breaches, unauthorized access, and misuse. In parallel, regulatory requirements for data protection and privacy have intensified, notably with frameworks such as the General Data Protection Regulation (GDPR [4, 20]), further complicating compliance for individual practitioners who lack institutional support. Current market solutions, including general-purpose secure messaging platforms like ProtonMail [19] and Signal [13, 14] as well as healthcare-specific platforms such as Doctolib [6] and MSSanté [10, 12], frequently fall short, either due to their complexity, high costs, or insufficient alignment with the comprehensive set of legal, technical, and user-centric requirements essential for both compliance and practical usability. The governance of healthcare data protection in Europe is characterized by a comprehensive set of regulations meticulously designed to ensure the confidentiality, integrity, and traceability of sensitive medical information. The cornerstone regulation, GDPR, establishes fundamental principles such as transparency, lawfulness, fairness in data processing, data minimization, and the implementation of robust technical and organizational measures to protect personal data. GDPR further requires explicit user consent and mandates prompt notifications (within 72 hours) in the event of data breaches (Articles 5, 32, and 33 [1–3]). In France, the "Code de la Santé Publique" (CSP [18]) supplements GDPR requirements by explicitly mandating the storage of healthcare data by certified Health Data Hosts (HDS, Article L1111-8 [16]), enforcing medical secrecy (Article L1110-4 [15]), and defining mandatory retention periods for medical records (a minimum of 20 years after the last treatment, Article R1112-7 [17]). Furthermore, the French National Commission for Information Technology and Civil Liberties (CNIL [5]) has established specific guidelines emphasizing data encryption at rest

and in transit, multi-factor authentication (MFA), comprehensive logging, and systematic non-repudiation measures. The "Politique Générale de Sécurité des Systèmes d'Information de Santé" (PGSSI-S [7–9, 11]) is a complementary framework that reinforces the use of End-to-End Encryption (E2EE), regular audits, and stringent user authentication protocols. It is evident that this legal framework gives rise to several critical user-centric, security, and organizational requirements, including transparency and lawful processing, data minimization, robust encryption (E2EE), mandatory multi-factor authentication (MFA), compliance with HDS-certified hosting, comprehensive traceability and non-repudiation, adherence to legal retention periods, and clear and ergonomic management of user consent. In order to address the rigorous legal and technical constraints, we propose U-HealthSec, a robust, user-centric architecture integrating several advanced security features. U-HealthSec provides robust E2EE by employing AES-256-GCM encryption locally on client devices, ensuring that sensitive data remains protected throughout storage and transfer. Additionally, U-HealthSec incorporates asymmetric encryption via Elliptic Curve Cryptography (ECC) to securely share symmetric encryption keys among authorized users. The architecture incorporates mandatory multi-factor authentication (MFA), in conjunction with OAuth2 and encrypted PASETO tokens, to ensure robust user authentication. In strict compliance with French healthcare regulations, U-HealthSec ensures data hosting exclusively through certified HDS, aligning its hosting practices with ISO 27001 and ISO 27018 standards. The comprehensive traceability and non-repudiation of all actions are guaranteed through the meticulous logging of each user action in a secure PostgreSQL database. This ensures accountability and facilitates auditability as mandated by the GDPR, the CNIL guidelines, and France's Code de la Santé Publique. User-centric design is central to U-HealthSec. An intuitive interface enables the clear management of user consent and rights, facilitating straightforward consent revocation and definitive data deletion. This approach ensures adherence to the GDPR provisions regarding the right to be forgotten. Furthermore, U-HealthSec integrates Attribute-Based Keyword Search (ABKS) technology, enabling secure and privacy-preserving searches within encrypted data without necessitating server-side decryption. This enhancement is particularly beneficial in terms of security and user experience, catering specifically to healthcare professionals who may not possess specialized expertise in cybersecurity. Future development of U-HealthSec will explore additional cryptographic methods, including homomorphic encryption and Searchable Symmetric Encryption (SSE), to further strengthen its capabilities. Additional improvements under consideration include developing a secure mobile application, automated

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

womENCourage 2025, Braşov, Roumania

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.  
ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM  
<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

compliance dashboards, and advanced anonymization processes for secondary data use in research. Consequently, U-HealthSec offers a comprehensive, scalable, and accessible solution that closely aligns with regulatory obligations and practical user requirements. This development signifies a substantial enhancement in the secure and compliant exchange of sensitive healthcare data, particularly catering to professionals operating outside conventional healthcare infrastructures.

#### ACM Reference Format:

Ambre Journot, Karima Boudaoud, and Christian Delettre. 2025. Meeting Healthcare Security Standards: From Legal Requirements to Technical Implementation. In *Proceedings of 12th ACM Celebration of Women in Computing: womENCourage™ 2025 (womENCourage 2025)*. , 2 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

#### References

- [1] CNIL. 2018. *Article 33 - Notification à l'autorité de contrôle d'une violation de données à caractère personnel*. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33> Consulté en mai 2025.
- [2] CNIL. 2023. *Article 32 : Sécurité du traitement*. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article32> Consulté le 9 mai 2025.
- [3] CNIL. 2023. *Article 5 : Principes relatifs au traitement des données à caractère personnel*. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5> Consulté en mai 2025.
- [4] CNIL. 2023. *Le règlement européen sur la protection des données*. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees> Consulté le en mai 2025.
- [5] CNIL. 2025. *Site officiel de la CNIL*. <https://www.cnil.fr/fr> Consulté en mai 2025.
- [6] Doctolib. 2025. *Confidentialité des données de santé chez Doctolib*. <https://www.doctolib.fr/sante/confidentialite/> Consulté en mai 2025.
- [7] Agence du numérique en santé. 2018. *PGSSI-S – Politique Générale de Sécurité des Systèmes d'Information de Santé (document du 28 mai 2018)*. [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/180528\\_PGSSI-S\\_0.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/180528_PGSSI-S_0.pdf) Consulté en mai 2025.
- [8] Agence du numérique en santé. 2023. *Fiche pratique : Référentiel d'Identité Électronique (v4)*. [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/231002\\_rie-fiche-pratique\\_v4-%281%29.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/231002_rie-fiche-pratique_v4-%281%29.pdf) Consulté en mai 2025.
- [9] Agence du numérique en santé. 2025. *Corpus documentaire PGSSI-S*. <https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire> Consulté en mai 2025.
- [10] Agence du numérique en santé. 2025. *MSSanté – Messagerie Sécurisée de Santé*. <https://esante.gouv.fr/produits-services/mssante> Consulté en mai 2025.
- [11] Agence du numérique en santé. 2025. *PGSSI-S – Politique Générale de Sécurité des Systèmes d'Information de Santé*. <https://esante.gouv.fr/produits-services/pgssi-s> Consulté en mai 2025.
- [12] Agence du numérique en santé. 2025. *Référentiel socle MSSanté v2*. [https://esante.gouv.fr/espace\\_documentation/mssante-clients-de-messageries-securisees-de-sante/referentiel-socle-mssante-2](https://esante.gouv.fr/espace_documentation/mssante-clients-de-messageries-securisees-de-sante/referentiel-socle-mssante-2) Consulté en mai 2025.
- [13] Signal Foundation. 2025. *Signal - Messagerie privée et sécurisée*. <https://signal.org/fr/> Consulté en mai 2025.
- [14] Signal Foundation. 2025. *Signal Protocol Documentation*. <https://signal.org/docs/> Consulté en mai 2025.
- [15] Légifrance. 2025. *Article L1110-4 du Code de la santé publique*. [https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000043895798](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043895798) Consulté en mai 2025.
- [16] Légifrance. 2025. *Article L1112-8 du Code de la santé publique*. [https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000033862549](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549) Consulté en mai 2025.
- [17] Légifrance. 2025. *Article R1112-7 du Code de la santé publique*. [https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000036658351/](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036658351/) Consulté en mai 2025.
- [18] Légifrance. 2025. *Code de la santé publique*. [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006072665/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072665/) Consulté en mai 2025.
- [19] Proton Mail. 2025. *Sécurité de Proton Mail*. <https://proton.me/fr/mail/security> Consulté en mai 2025.
- [20] Ministère de l'Économie. 2023. *Règlement général sur la protection des données (RGPD)*. <https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd> Consulté en mai 2025.