Integrated Knowledge Management (IKM) Volume 10

Version 1 - Last Updated 2/20/2024

Table of Contents

Part I. Patient Data Privacy

1. Patient Data Privacy

1.1. Important of Patient Data Privacy

Patient data privacy refers to patients' legal protection of their personal health information by healthcare providers. All healthcare professionals must protect the confidentiality and integrity of patients' health information, while simultaneously providing patients access to their data, including medical histories, test results, treatments, and other personal information collected during patient interactions. Patient data privacy stems from the branch of medical ethics that focuses on doctor-patient confidentiality and is critical for building trust and ensuring patients feel confident disclosing important information about their health. As well as having access to their data, patients also have the right to correct any errors in their record and to allow others to access their health data. These rights are protected both by the medical code of ethics and the law, with violations leading to legal penalties. Several laws exist in the United States and abroad to advance patient data privacy, including the following:

• Health Insurance Portability and Accountability Act (HIPAA) (United States) [1]: Protects the confidentiality, integrity, and accessibility of health information. HIPAA provides patients with a legal right to access and receive copies of their personal health data upon request and is broken down into Privacy, Security, and Breach Notification Rules:

Privacy Rule: The Privacy portion of HIPAA dictates that health care providers and health plans must provide access to protected health information (PHI) in "designated record sets". These record sets are maintained by the provider and contain all information collected or stored by the healthcare entity, including paper records, data in electronic systems, remote/archived information, or data pertaining to where the PHI originated. It also ensures that patients can access and edit their records if they find an error. [2]

Security Rule: Healthcare providers must enact safeguards to protect PHI and ensure that PHI data is not improperly disclosed. Several measures including access control tools, encryption, and audit trails are types of security measures that can be built into systems containing PHI.

Breach Rule: Federal law requires doctors, hospitals, and other health care providers to notify patients and the Secretary of Health and Human Services if a breach of PHI security occurs. If a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction.

• 21st Century Cures Act Information Blocking Rule [3]: Prohibits health information technology vendors from blocking exchange of health information or restricting patient access to such information. The information blocking rule within this act is of particular importance to patients because it includes provisions ensuring that patients can electronically access all their electronic health information (EHI), structured and/or unstructured, at no cost, and with the application of their choice. Patients have the recourse to report information blocking by healthcare systems and other vendors. [4]

• Coronavirus Aid, Relief, and Economic Security Act : Advanced data privacy for patients' Substance Use Disorder (SUD) records and mandated that Health and Human Services (HHS) issue guidance during the COVID-19 Pandemic regarding sharing patients' protected health information (PHI). [5]

• General Data Protection Regulation (GDPR): An EU policy that safeguards all personal data including healthcare data. It grants patients' rights over their data and mandates healthcare organizations provide data protection measures. This policy extends beyond the EU and protects EU citizens wherever they are globally. [6, 7]

Several key principles outline the GDPR approach to data protection:

o Lawfulness, fairness, and transparency

o Purpose limitation

o Data minimization

o Accuracy

o Storage limitation

o Integrity and confidentiality

1.2. Patient Data Privacy and IKM

IKM does not handle or store individual patient records, and therefore does not directly have authority over the security or dissemination of these records. IKM is a contributed knowledge management application that will serve as a quality care driver to improve healthcare data quality and support the downstream accuracy of patient treatments and public health decisions. The contributed IKM application provides a space for healthcare knowledge to be managed in a single centralized area and improves clinical support systems to help healthcare providers. While IKM does not directly handle or store individual patient records, it plays a vital role in preserving the integrity and quality of healthcare data that are transferred within and between systems in the healthcare labyrinth.

1.2.1. HIPAA v. GDPR and Patient Data Privacy

Health Insurance Portability and Accountability Act (HIPAA) is a law designed specifically to protect individuals' medical information while General Data Protection Regulation (GDPR) is a broader regulation that encompasses protection of various types of personal data, including health data. However, both laws protect an individual's right to the safe and secure handling of their personal information and are designed to protect an individual's privacy.

HIPAA rules only apply to covered entities including health care providers, health plans, and healthcare clearinghouses. Below are examples of each covered entity [8]:

1. Healthcare provider: doctors, clinics, chiropractors, nursing homes, pharmacies

2. Health plans: health insurance companies, HMOs, company health plans, Medicare/Medicaid

3. Healthcare clearinghouse: entities that process nonstandard health information received from another entity into a standard.

GDPR rules apply to "Controllers" and "Processors". Controllers are typically the same as HIPAA Covered Entities, and generally *collect* personal information, whereas a Processor is similar to the HIPAA business associate and usually *processes* personal information. Unlike HIPAA, GDPR has extraterritorial reach to locations outside of the EU where EU persons personal information is in use.

Most relevant to IKM is the GDPR rules that extend extraterritorial reach to personal data "processors" in the United States when the controller is in the EU, and has heightened protections for data concerning health, genetics, or biometrics. US healthcare providers can satisfy the GDPR security requirements for electronic personal data by complying with the HIPAA Security Rule or by following the security framework of the National Institute of Standards and Technology (NIST) (from which the HIPAA Security Rule is based).

Although IKM does not qualify under HIPAA as a covered entity, nor under GDPR as a controller or processor, IKM values patient data privacy and upholds the highest security standards. [9]

1.3. Understanding Different Entities and Their Roles in Patient Data Privacy

SNOMED CT® and LOINC® are similar to IKM as they do not directly handle patient data nor collect any PHI. Below are SNOMED CT® and LOINC®'s commitment to data privacy:

1.3.1. SNOMED CT®

SNOMED CT®'s statement on data privacy [10]:

SNOMED CT® itself doesn't directly handle patient data privacy. However, it contributes indirectly to patient data privacy by providing a standard language for clinical data. SNOMED International Services provides a detailed description of Personal Data processed for the purposes of Analytics, Contacting the User, Hosting and other uses. The privacy policy also provides details of an individual's rights to their data and how to access and control personal information, and even includes a point of contact for questions specifically concerning privacy.

1.3.2. LOINC®

As LOINC's privacy policy states, LOINC does not collect any personal health information. LOINC® is a catalog of measurements that includes laboratory tests and clinical measures, that are not limited to vital signs and anthropometric measures, and standardized survey instruments. LOINC® also contains codes for the collection types for these items, such as panels, forms, and documents. [11]

1.4. Conclusion

Patient data privacy is an important aspect of delivering safe and effective healthcare and is protected by HIPAA and other laws. The EU's General Data Privacy regulation ushered in an era of stringent and protective data privacy standards and have even influenced new policies, such as the California Consumer Privacy Act (CCPA). [12] As we navigate the complexities of data privacy regulations, our team remain committed to protecting patient data and patient privacy. Though not directly governed by HIPAA or GDPR, we believe patient data privacy should remain at the forefront of our operations, reinforcing our commitment to quality healthcare.

1.5. References

1. HIPAA Guide. HIPAA Updates [Internet]. Available from: https://www.hipaaguide.net/hipaa-updates/

2. U.S. Department of Health & Human Services. Privacy, Security, and Electronic Health Records [Internet]. Washington (DC): HHS;. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

3. 21st Century Cures Act Information Blocking Rule" [Internet]. Available from: https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/

4. Office of the National Coordinator for Health Information Technology (ONC). Information Blocking [Internet]. Available from: https://www.healthit.gov/topic/information-blocking

5. Congress. Care Act [Internet]. Washington, DC: Congress; 2020. Available from:

https://www.congress.gov/bill/116th-congress/house-bill/748

6. GDPR.eu. General Data Protection Regulation (GDPR) [Internet]. Available from: https://gdpr.eu/what-is-gdpr

7. GDPR Advisor. GDPR Compliance in the Healthcare Industry: Protecting Patient Data [Internet]. Available from: https://www.gdpr-advisor.com/gdpr-compliance-in-the-healthcare-industry-protecting-patient-data/

8. U.S. Department of Health & Human Services. Covered Entities and Business Associates [Internet]. Available from: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

9. The National Law Review. Does GDPR Regulate Clinical Care Delivery for US Health Care Providers [Internet]. Available from: https://www.natlawreview.com/article/does-gdpr-regulate-clinical-care-delivery-us-health-care-providers#:~:text=Unlike the HIPAA Privacy Rule which makes obtaining,another lawful basis for processing the Personal Data.

10. Iubenda. Privacy Policy [Internet]. Italy: iubenda; Available from: https://www.iubenda.com/privacy-policy/46600952

11. LOINC. Privacy Policy [Internet]. Available from: https://loinc.org/privacy-policy/

12. Deloitte. CCPA Compliance and Readiness [Internet]. Available from: https://www2.deloitte.com/us/en/pages/advisory/articles/ccpa-compliance-readiness.html