The Legal Implications of Healthcare Data Management in the Digital Age

Rifa Safeer Shah

LAW 371

Table of Contents

Abstract

With the rise in the amount of data that is being generated, consumed, and shared, it has become essential to have a proper system for healthcare data management. A complex network of legal and ethical standards governs this process, aiming to safeguard patient privacy while supporting efficient health care delivery and advancing public health efforts. This paper examines the legal implications of healthcare data management, focusing on data privacy, ethical considerations, and the impact of utilizing emerging technologies.

Introduction

In our current times, hospitals and the healthcare industry rely on internet tools and applications to track patient information and their medical data accurately. This data is now managed centrally using electronic health records (EHRs), which enable hospital staff to easily document patient data and allow patients to access their data. Some popular EHR systems used by hospitals and medical centers are Epic Systems, Cerner, NextGen Healthcare, and AtenaHealth. These systems offer a strong and well-rounded framework that enables hospital staff and patients to access health data more efficiently, enhancing interoperability and supporting compliance with existing federal and state health information laws and policies.

Challenges in Data Sharing

When working with data, it is important to have accurate and authentic information. Data sharing in healthcare requires the sharing of patient data among providers, public health agencies, and external vendors to promote interoperability and provide specialized patient care. However, this comes with a lot of challenges related to privacy and the security of the data and the identity of people. Laws and regulations like the HIPAA and state privacy rules can often be overlooked and contradict each other. Different hospitals also use different computer systems that don't work well together, making it hard to share information. It is essential to properly maintain patient charts, which include immunization records, diagnosis information, and lab results, so they can be tracked appropriately, and the patient can have a seamless experience during their care.

Ethical Considerations

Healthcare data management is not only about following the laws and regulations, but it also focuses on including the patient in the entire process and keeping them aware of their

information. This means providing the patients' details about how their information will be used and requesting permission before sharing with third parties. Individuals accessing and working with sensitive data are responsible for keeping this information private and safe by ensuring appropriate access is granted and data sharing is limited or monitored for safety reasons.

Emerging Technologies and Data Privacy

To help with maintaining proper safety of patient data and also ensuring effortless transition of their patient care, most hospitals and medical facilities now use an EHR system. This allows for ease of use on the patient side by allowing them to access all of their information in one portal rather than different portals or printed charts. It also provides a better system for providers and hospital staff to give better and holistic care to patients by providing quick access to their previous diagnoses, allergies, and medical conditions. EHRs help address the security and privacy concerns faced with the traditional bookkeeping of sensitive health information. They also provide a layer of added security information is not leaked or accessed without permissions.

Laws and Policies

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act provides a baseline for healthcare data protection standards. It mandates that healthcare and medical facilities must implement safeguards to ensure the confidentiality and security of PHI. Even though they are federally implemented laws, some states have added their complementary privacy regulations to further safeguard sensitive information.

21st Century Cures Act, Electronic Health Information (EHI)

The 21st Century Cures Act defines Electronic Health Information (EHI) as any electronic health data that’s part of a person’s medical record and used to make decisions about their care. This includes patient medical information like diagnosis information, immunization records, clinic notes, imaging reports, lab results, and billing and insurance information.

Information Blocking and EHI Exception Rules

The ONC Cures Act Final Rule states that healthcare providers and IT staff are prohibited from engaging in information blocking, which basically means restricting access and

sharing of electronic health information to appropriate individuals requesting this information.

Even though it is required to comply with the information blocking rule, there are some exceptions to this for data privacy and security reasons. These exceptions are classified into two categories: exceptions that involve not fulfilling the request to access, exchange, or use EHI, and exceptions that involve procedures for fulfilling the requests to access, exchange, or use EHI. The eight exceptions include: the Preventing Harm Exception, the Privacy Exception, the Security Exception, the Infeasibility Exception, the Health IT Performance Exception, the Content and Manner Exception, the Fees Exception, and the Licensing Exception.

Information Blocking Exceptions

1. **Preventing Harm Exception** – restricting access, exchange, or use of EHI is allowed if it prevents harm to a person.
2. **Privacy Exception** – restricting access, exchange, or use of EHI is allowed to protect an individual's privacy based on applicable privacy laws and patient approval.
3. **Security Exception** – restricting access, exchange, or use of EHI is allowed in order to safeguard the security of the information.
4. **Infeasibility Exception** – restricting access, exchange, or use of EHI is allowed if the request cannot be fulfilled due to technical limitations or legal restrictions.
5. **Health IT Performance Exception** – restricting access, exchange, or use of EHI is allowed in order to maintain or improve the performance of health information technology.
6. **Content and Manner Exception** – restricting access, exchange, or use of EHI is allowed if the request cannot be completely fulfilled, and some specific conditions might need to be implemented to support interoperability and maintain fairness.
7. **Fees Exception** – restricting access, exchange, or use of EHI is allowed to be able to charge a fee that results in a reasonable profit margin.
8. **Licensing Exception** – restricting access, exchange, or use of EHI is allowed in order to license interoperability elements.

Information Blocking Legal Impacts

Any violations of the Information Blocking Rules result in a hefty fine of up to $1 million per violation for healthcare IT staff. Additionally, healthcare providers may face a loss of federal benefits or support from health programs. Hence, it is very important for facilities to have robust workflows to monitor and triage EHI requests while providing a clear and timely response to the requestor.

Center for Health Information and Analysis (CHIA)

The Center for Health Information and Analysis (CHIA) is an agency that manages healthcare data. The main focus of this agency is to collect, analyze, and publish information related to how healthcare is being used, the costs related to it, and its performance. These rules ensure the data is accurate, secure, used properly, and accessible to the public when required.

Identity and Access Management

In healthcare, IAM systems are crucial to ensure that only authorized individuals have access to sensitive patient data. Having these protocols in place ensures that data is always accessed by the appropriate individuals and kept safe. Implementation of EHRs in a hospital workflow helps with maintaining access and tracking of data, which further helps with being compliant with legal mandates and other regulatory requirements.

Some best practices to implement include:

- **Role-Based Access Control (RBAC)** – where users are granted access based on their role within the hospital or organization.
- **Multi-Factor Authentication (MFA)** – added security to ensure authentic access to confidential information.
- **Audits and Reporting** – ensures that the hospital and facility have detailed logs of who, what, and when regarding the confidential information.

Conclusion

It is important for anyone working with EHRs or managing this data to be aware of federal and state laws while also maintaining ethical considerations. The use of EHR systems ensures that the policies and regulations put in place are being followed throughout the facility and the patient care process. The challenges that traditional hospital processes and workflows face with information security are elevated with the implementation of EHR systems while improving the overall process of seeking medical care.

Appendix

Research Paper Outline

- Abstract
- Introduction
- Identity and Access Management
- Conclusion

References

Cures Act Final Rule, Information Blocking Exceptions, Cures Act Final Rule: Information Blocking Exceptions

Interoperability and Patient Access Final Rule, CMS Interoperability and Patient Access Final Rule (CMS-9115-F) | CMS

Summary of the HIPAA Privacy Rule, Summary of the HIPAA Privacy Rule | HHS.gov

Center for Health Information and Analysis (CHIA), About the Agency

Ensuring Patient Privacy: Ethical Considerations in Healthcare Data Management, "Preserving Patient Trust: Navigating the Ethical Landscape of Healthcare Data Management in the Digital Age"