HealthTechWiz

The Role Of Information Privacy In The New Healthcare Environment

The benefits of digital health and improved patient experience are infinite; however, a lot of patient-sensitive information is exchanged in the process. Therefore, it is driving the need for ensuring privacy and promoting more effective communication between physicians and patients than ever!

BY HEALTHTECHWIZ

Atlanta

7000 Central Parkway,
Suite 220, Atlanta, GA 30328
(678) 648-7722

00 table of content

Foreword 03

Understanding The Importance Of Healthcare Privacy 04

Patient Privacy: Medical Data Breaches Each Year 05

Medical Privacy Ethics - What does it mean? 06

Protecting Patient Privacy 07

Maintaining Patient Confidentiality 08

Health Information Privacy & HIPAA 09

Healthcare Interoperability: Privacy & Security 11

Transparency 12

Secondary Uses of Personal Health Information 13

Privacy in the Real World: Trends and Considerations 14

Foreword

Many health information technology improvements have enhanced healthcare quality and patient experience, boosted health information for treatment, and enforced safeguards that cannot be applied quickly or cost-effectively to paper-based health records.

Today, sensitive health information in digital form is aggregated, used, and shared more efficiently. Nevertheless, the digitization of health data also presents new concerns and privacy risks. On the other hand, the soaring cost of healthcare efficiency may pave the way for incentives to use the data in new ways.

While everyone appreciates the potential value of health information exchange and technological advancements, many experts and organizations are concerned about sensitive health information safety. Therefore, it is essential for ensuring public trust.

According to research, the public sees the potential value of health information exchange and technological advancements; on the other hand, it also remains gravely concerned about the privacy of their sensitive health information. Therefore, ensuring public trust will be crucial to implementing nationwide health information exchange, and it is becoming more than necessary in these times.

Understanding The Importance Of Healthcare Privacy

Privacy is a fundamental human right that underpins freedom of expression, thought, association - freedom from interference, intrusion, or discrimination.

Information privacy in the evolving healthcare environment is critical for both the patients and the healthcare practitioners.

Healthcare privacy establishes boundaries to limit access to communication and information. Confidentiality plays a crucial role in building trust between patients and medical professionals. When confidence builds, patients willingly disclose their health information to healthcare practitioners.

As a result, trust-based physician-patient relationships can lead to better interactions and higher-quality health visits.

Patient Privacy: Medical Data Breaches Each Year!

According to the U.S. Department of Health and Human Services:

- 2019, 2020, and the first seven months of 2021 reported 827 healthcare breaches.
- 50+ million people had their medical records compromised.

Type of breach 2019-2021

Hacking or IT Incident	605
Unauthorized Access or Disclosur	165
Theft	30
Loss	16
Improper Disposal	11
Total	**827**

The ten most significant data breaches involved nearly 19 million records.

Medical Privacy Ethics - What does it mean?

Medical privacy ethics demands maintaining a patient's personal and medical information secret. Therefore, all confidential information and correspondence are between the doctor, the physician, the patient, the healthcare provider, or the health insurance company. Similarly, information related to the treatment should be protected at all costs and cannot be disclosed to anyone without their consent.

In the highest regard, a patient's medical information is only shared with the given health care provider. It shall not divulge to others unless the patient's consent to disclose such information to others is provided.

A patient's confidentiality should be maintained because the communication of personal information or records may create personal or professional problems. In contrast, patients depend on doctors to keep their medical information private.

Though it is rare to keep the medical records or information completely undisclosed, the widespread breach of confidentiality happens when the doctors pass the medical information to others and refer to it as one of their case studies. If this information gets published in professional journals, the patient's identity is never disclosed, and if it appears in any way, the patient has the right to sue.

There are many rights which the patient has and can duly exercise.

Here are a few:-

- Right to Appropriate Humane Treatment and Medical Care
- Right to Information
- Right to Choose Health Care Facility and Provider
- Right to Medical Records, Privacy, and Confidentiality

Protecting Patient Privacy

Any healthcare provider in the U.S. is predominantly focused on keeping people healthy —not securing data networks. However, the truth is millions of medical records are hacked, and a HIPAA-related data breach costs providers an average of $715,000. This has been happening since the maintenance of digitized patient records.

It is a daunting task to protect patient privacy, but complying with HIPAA security rules is a never-ending critical mission. The four basic yet essential ways to safeguard patient information are:

1. Build a security culture in the organization
2. Perform a security risk assessment
3. Create a PHI security improvement plan
4. Encrypt all patient data

Maintaining Patient Confidentiality

Patient privacy and confidentiality are fundamental to the U.S. healthcare system. Protecting the personal information entrusted to medical professionals is part and parcel of the job.

Here is how healthcare organizations can be sure that they keep information appropriately protected at all times.

- Build to scale policies and confidentiality agreements
- Provide regular training
- Ensure data is stored on secure systems.
- No mobile phones
- Avoid circulation of printed material

As the size of the patient data grows, so does the size of the security threat. There are more requirements to connect different parts of the healthcare system in the new digital medical age to create seamless experiences for both parties.

Health Information Privacy & HIPAA

HIPAA - Health Insurance Portability and Accountability Act establishes the standard for sensitive patient data protection. Organizations that work with protected health information (PHI) must process security measures and follow them to ensure HIPAA Compliance.

Why was the Health Insurance Portability and Accountability Act established?

- The statute focuses on creating confidentiality systems within and beyond healthcare facilities.
- The goal of keeping protected health information private.

HIPAA Cover

- Healthcare facility or private office personnel
- Students
- Health plans (e.g., insurance companies)
- Billing companies
- Non-patient care employees
- Electronic medical record companies

Primary HIPAA Goals

- "Need To Know" - by limiting the use of protected health information
- Penalize the ones who do not comply with confidentiality regulations.

Protected Health Information

- Specific patient identifier to healthcare information (name, social security number, telephone number, email address, street address, among others)

HIPAA Privacy Rules

- It foresees how patient data is used within a healthcare facility
- How the data is communicated outside a health care facility
- For the disclosure: Patients must provide a signed consent

HIPAA Protected Data

- Written, paper, spoken, or electronic data
- Transmission of data within and outside a health care facility
- Applies to anyone or any institution involved with the use of healthcare-related data
- Data size does not matter

Types of Electronic Devices

- Both hardware and software

Healthcare Interoperability: Privacy & Security

Ever since the 2009 Health Information Technology for Economic and Clinical Health Act came into effect, it has promoted strong privacy and security practices. The significant adoption of health IT has heavily impacted the nature of sharing health data. It is anticipated to double the CMS Interoperability, Patient Access Rule, and ONC Cures Act, Final Rule in the longer run.

- The CMS and ONC rules together provide a regulatory framework for the patient access to and sharing of EHI.
- Patients can decide with whom they will share EHI.
- Organizations developing APIs and health IT systems and applications must act now to define the scope and extent of necessary readiness efforts.
- HIPAA-covered entities and BAs and third-party app developers not subject to HIPAA should immediately undertake readiness initiatives to identify gaps in technologies, governance, and operations relative to the new requirements and determine appropriate updates to design engineering and functions of the technologies and compliance programs.

Transparency

- Third-party health apps are a significant concern in the context of the CMS and ONC rules.
- The apps and providers are generally not highly regulated yet and can continue collecting and sharing health data improperly.
- To alleviate these concerns, app developers should implement standard privacy safeguards.
- The Health Insurance Portability and Accountability Act provides details of how their EHI is accessed, processed, shared, or sold.
- It should also provide transparency into the system or application's capabilities, including accessing other information on the patient's device and disabling such access.

Secondary Uses of Personal Health Information

There has been some confusion about when identifiable personal health information can be used for secondary purposes. Basically, health information is used for secondary purposes namely:

- Health system planning
- Public health monitoring
- Program evaluation and research
- Management
- Quality control

Sometimes health information will be "de-identified" or "anonymized" before it is used for these secondary purposes.

Privacy in the Real World: Trends and Considerations

Healthcare data has been increasing. With this, the benefits accompanying innovations and advances in computing technology, such as those stemming from artificial intelligence and machine learning, are increasingly relevant to a growing number of healthcare organizations.

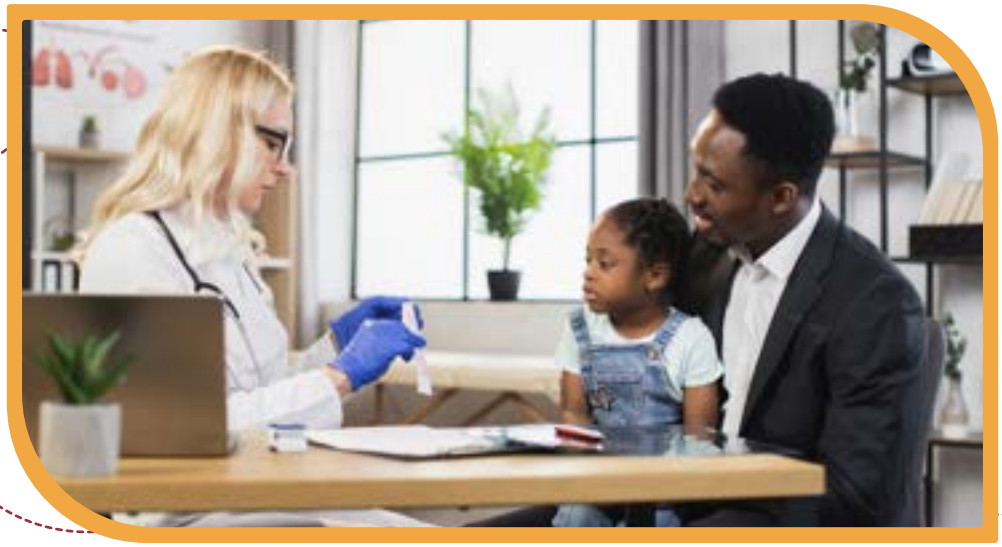
Recently developed privacy-enhancing technologies and methods are being touted as possible solutions to mitigate privacy risks associated with inadvertent disclosure and guard against sinister data incursions resulting from cybercrime.

Well, the good news is...

- By 2023, 64% of the world's population will have its personal information covered under current privacy regulations, up from 10% today.
- By year-end 2022, more than 1 million organizations will have appointed a privacy officer (or data protection officer).

Ultimately, before moving forward with any Healthcare Privacy or other privacy-enhancing technologies. The personnel need to collaborate and carefully explore the consequences of the data protection measures.

Additional resources and effort should be dedicated to carefully evaluating privacy protections for patient-level data in various public and private scenarios. Failure to do so will likely result in more frequent and severe cybercrime breaches of critical infrastructure and significant privacy implications for individuals and groups whose data is widely available and easily accessible.



HealthTechWiz

About HealthTechWiz

At HealthTechWiz, we are passionate about the healthcare industry's progress through extensive industry know-how and breakthrough technology. From healthcare providers to Pharma/Life Sciences organizations, we look forward to serving everyone enthusiastic and focused on adopting new technologies. Our custom healthcare solution will help your business agility and accelerate responding to immediate business needs.

As Healthcare software providers, we're really good at - Custom Healthcare solutions, Healthcare Software Solutions, and Healthcare software development.

Atlanta,

7000 Central Parkway, Suite 220,
Atlanta, GA 30328

Phone: (678) 648-7722
Email: contactus@healthtechwiz.com

HealthTechWiz