HIPPA COMPLIANCE

After reading this factsheet you should:

- Understand the key requirements in HIPAA compliance.
- Know the benefits to HIPAA compliance.

What is HIPAA Compliance?

HIPAA (Health Insurance Portability and Accountability Act) is a United States federal law passed in 1996 that establishes nationwide standards for the protection of sensitive health information. HIPAA is administered by the U.S. Department of Health and Human Services Office for Civil Rights (HHS). HIPAA compliance entails complying with the rules provided in this act. The main objective of HIPAA is protecting the privacy and security of patients protected health information (PHI) while enabling the safe exchange of health data for things like healthcare operations, payment, and treatment.

Who do HIPAA rules apply to?

HIPAA rules apply to covered entities and business associates. A covered entity is a health care provider, a health plan, or a health care clearinghouse. A list of each of these covered entities can be found here. If a covered entity engages with business associates to execute its health care duties and responsibilities, they must ensure that they comply with HIPAA regulations. Examples of business associates include IT support firms, cloud storage providers and billing companies.

What are the key requirements in HIPAA compliance?

To describe patient rights and provider obligations, the HHS established basic rules:
Privacy Rule: Protects all “individually identifiable health information” held or communicated in any format, including electronic, written, or oral, by a covered entity or a business associate. According to the Privacy Rule, this data is referred to as "protected health information (PHI)". It gives individuals authority over their PHI, including the right to access and manage it.

The confidentiality of PHI must be protected by policies and procedures in place at covered entities. The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

Security rule: Organisations are required to put security measures in place to safeguard the privacy and confidentiality of patient information, particularly electronic PHI (ePHI). Administrative, physical, and technological protections must be put in place by covered entities to prevent unauthorised access to, use of, or disclosure of ePHI.

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164. Security risk assessment tool found here.

Breach notification rule: Following a breach of unsecured protected health information, HIPAA covered companies and their business associates are required to notify the affected individuals, the Department of Health and Human Services (HHS) and in some situations, the media. Depending on whether a breach affects 500 people or fewer, a covered entity has different breach notification responsibilities. The breach notification rule is located 45 CFR Part 164.400-414.
Enforcement rule: Establishes processes for looking into HIPAA infringement claims and specifies fines for non-compliance. The enforcement rule is located at 45 CRF Part 160, Subparts C, D and E.
Transactions rule: Health care information is transferred through transactions. A health plan or healthcare provider must adhere to the standard if they do one of the identified transactions.

Identifiers rule: Also known as the National Provider Identifier (NPI) Rule, provides healthcare providers, health plans, and other organisations involved in healthcare transactions a unique identification number.

What public health information is protected by HIPAA?

Protected health information includes the following categories of data:

- Physical and mental health: Data on past, present, and future physical and mental health.
- Treatment: Information about the delivery, organisation, or management of healthcare and healthcare services.
- Payment information: Information pertaining to the payment for medical services, such as billing data, insurance details, and claims details.
- Identifiers: Anything that can be used to identify the subject of the information

What are the benefits of HIPAA compliance?

- Patient Privacy Protection: Disclosure of patient information is limited leading to a reduction in information breaches and encouraging confidentiality and trust in patient contacts.
- Enhanced Security Measures: The security framework to protect ePHI is strengthened.
- Legal and Reputational Compliance: Assists covered entities in complying with legal obligations and avoiding possible legal actions.
- Interoperability and Information Exchange: Safe electronic data sharing between covered entities, resulting in improved patient care coordination and effective healthcare operations.

Can a covered entity disclose PHI without the individual's permission?

There are a limited number of circumstances where the law permits a covered entity to disclose PHI without the individual permission. These circumstances can be found here.

What are the steps to achieve HIPAA compliance?

1. Perform a risk assessment: Identify any potential dangers to the confidentially.
2. Create policies and guidelines: Address topics such as access restrictions, workforce training, incident management, privacy, security, and breach response.
3. Apply safeguards: Protect PHI by putting in place the necessary safeguards.
4. Workforce training: Briefings on policy changes, and instruction on how to handle PHI.
5. Business Associate Agreements (BAAs): Must follow HIPAA regulations.
6. Conduct audits and surveillance.
7. Create a breach response strategy.
8. Maintain documentation..

A HIPAA compliance checklist can be seen here.

Health Innovation Hub Ireland
info@hih.ie
www.hih.ie

HIHI (UCC)
Western Gateway Building
University College Cork
Cork, Ireland
+353 (0)21 420 5560

HIHI (TCD)
H&H Building
St James' Hospital
Dublin 8, Ireland
+353 (0)1 896 2573

HIHI (University of Galway)
Lambe Institute
National University of Ireland
Galway, Ireland
+353 (0)91 492 072

HIHI (MTU)
CREATE Building
Munster Technological University
Cork, Ireland
+353 (0)21 432 6758