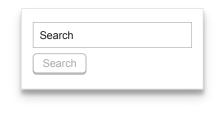HIPAA
JOURNAL

HIPAA Compliance News »   GDPR Compliance News »   Practical HIPAA »   HIPAA Compliance Checklist   HIPAA Laws »   About HIPAA Journal

What is Considered Protected Health Information Under HIPAA?

Home   **HIPAA Compliance News**   What is Considered Protected Health Information Under HIPAA?

Search

Search

Posted By HIPAA Journal on Apr 2, 2018

Share this article on:

f   **Facebook**   🐦 **Twitter**   in **LinkedIn**

Protected health information – or PHI – is often mentioned in relation to HIPAA and healthcare, but what is considered protected health information under HIPAA?

What is Considered Protected Health Information Under HIPAA Law?

If you work in healthcare or are considering doing business with healthcare clients that requires access to health data, you will need to know what is considered protected health information under HIPAA law. The HIPAA Security Rule demands that safeguards be implemented to ensure the confidentiality, integrity, and availability of PHI, while the HIPAA Privacy Rule places limits the uses and disclosures of PHI.

Violate any of the provisions in the HIPAA Privacy and Security Rules and you could be financially penalized. There are even criminal penalties for HIPAA violations. Claiming ignorance of HIPAA law is not a valid defense.

Under HIPAA, protected health information is considered to be individually identifiable information relating to the health status of an individual, the provision of healthcare, or individually identifiable information that is created, collected, or transmitted by a HIPAA-covered entity in relation to payment for healthcare services.

Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and

demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. PHI relates to physical records, while ePHI is any PHI that is created, stored, transmitted, or received electronically.

PHI only relates to information on patients or health plan members. It does not include information contained in educational and employment records.

PHI is only considered PHI when an individual could be identified from the information. If all identifiers are stripped from health data, it ceases to be protected health information and the HIPAA Privacy Rule's restrictions on uses and disclosures no longer apply.

Data Elements that Allow Patients to be Identified

PHI is any health information that includes the following 18 identifiers. If these identifiers are removed the information is considered de-identified protected health information, which is not subject to HIPAA Rules.

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

How Must Health Information be Protected?

The HIPAA Security Rule requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI, although HIPAA is not technology specific and the exact safeguards that should be implemented are left to the discretion of the covered entity.

HIPAA requires physical, technical, and administrative safeguards to be implemented. Technologies such as encryption software and firewalls are covered under technical safeguards. Physical safeguards include keeping physical records and electronic devices containing PHI under lock and key. Administrative safeguards include access controls to limit who has access to PHI and security awareness training.

Author: HIPAA Journal

Share This Post On

About HIPAA Journal

HIPAA Journal provides the most comprehensive coverage of HIPAA news anywhere online, in addition to independent advice about HIPAA compliance and the best practices to adopt to avoid data breaches, HIPAA violations and regulatory fines. HIPAA Journal's goal is to assist HIPAA-covered entities achieve and maintain compliance with

Recent News

- Microsoft ADFS Vulnerability Allows Bypassing of Multi-Factor Authentication

- Vulnerabilities in Patient Monitors Allow Vital Signs to be Altered in Real Time

- Vulnerabilities in Fax Machines Can Be Exploited to

state and federal regulations governing the use, storage and disclosure of PHI and PII.

Gain Network Access and Exfiltrate Sensitive Data

▶ Lawmakers Accuse Oklahoma Department of Veteran Affairs of Violating HIPAA Rules

▶ APWG Detects 46% Rise in Phishing Websites in Q1 2018

Tweets by @HIPAAJournal

HIPAA Journal
@HIPAAJournal

A recent report from Black Book Research has revealed more than 90% of healthcare organizations have experienced a data breach since Q3 2016 bit.ly/2jZQL36

Healthcare IT Security Budg…
A recent report from Black Boo…
hipaajournal.com

3h

HIPAA Journal

Embed   View on Twitter

Advertising and Sponsorship   Submit Articles and Press Releases   Newsletter Subscription   Terms and Conditions   Privacy Policy   Site Map