Test your knowledge of the HIPAA PHI definition, what is considered PHI under HIPAA, and when it is allowable to disclose PHI without patient authorization.

What is PHI?

PHI is an acronym of Protected Health Information - a term used in the HIPAA Privacy Rule to describe individually identifiable health information held or transmitted by a HIPAA Covered Entity or a Business Associate in any form or media, whether electronic, paper, or oral.

There is a difference between individually identifiable health information/PHI and PII (Personally Identifiable Information) inasmuch as PII only becomes PHI when it is created, maintained, or received by a Covered Entity or Business Associate and relates to:

- An individual’s past, present, or future physical or mental health or condition,
- The provision of health care to an individual, or
- The past, present, or future payment for the provision of health care to an individual.

There are exceptions to this definition of PHI for Covered Entities and Business Associates that are educational institutions or employers. For example, individually identifiable health information covered by the Family Educational Rights and Privacy Act (FERPA) does not qualify as PHI, nor do employment records held by a Covered Entity in its capacity as an employer.

HIPAA Protected Health Information

HIPAA Protected Health Information consists of eighteen PHI identifiers that could be used alone or in combination with other reasonably available information by an anticipated recipient in order to identify an individual who is a subject of the information. The eighteen PHI identifiers are:

- Names (Full, or last name and initial).

Note: When an individual can be identified by the name of a relative, employer, or household member (i.e. “mother of...”), that information is also considered to be PHI.

- All geographical identifiers smaller than a state.

Note: Except for the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same first three digits contains more than 20,000 people. If the geographic unit contains 20,000 or fewer people, the zip code should be changed to 000.

- Dates (other than year) directly related to an individual.
Note: The dates category includes all element of dates (except year) relating to birth, death, admission, and discharge, and all elements of dates (including year) when the individual is aged over 89.

- Phone Numbers.

Note: Includes landlines, mobiles, and any phone numbers associated with relatives, employers, and household members that could reasonably identify the individual who is the subject of the information.

- Fax numbers.

Note: As above with regards to any fax numbers associated with relatives, employers, and household members that could reasonably identify the individual who is the subject of the information.

- Electronic mail addresses.

Note: While this category of PHI is generally considered to mean email addresses, it could also be reasonably inferred to relate to social media addresses and handles.

- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers (including serial numbers and license plate numbers)
- Device identifiers and serial numbers;
- Web Uniform Resource Locators (URLs) and Uniform Resource Identifiers (URIs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except unique codes assigned to the individual’s record to allow the re-identification of data after it has been de-identified.

Allowable Uses and Disclosures of PHI without Patient Authorization
As a best practice, Covered Entities should voluntarily obtain patient consent for uses and disclosures of PHI for treatment, payment, and health care operations. For most other uses and disclosures of PHI, it is necessary to obtain authorization from the patient.

Exceptions to this requirement exist. For example, it is allowable for a Covered Entity to disclose PHI to another Covered Entity (or another Covered Entity’s Business Associate) provided both parties have - or have had - a relationship with the patient, the PHI disclosed pertains to the relationship, and only the minimum necessary PHI is disclosed for the intended purpose.
The HIPAA Privacy Rule also permits use and disclosure of PHI without a patient’s authorization for public interest purposes and for benefit activity purposes. Again the minimum necessary standard applies, and the disclosure of PHI must be conducted in compliance with the HIPAA Security Rule. Allowable public interest and benefit activities include (but are not limited to):

- When required by law (including by statute, regulation, or court order).
- When required by public health authorities to prevent or control the spread of a disease.
- To report child abuse, neglect, or domestic violence to the appropriate authorities.
- When an employer requires information to comply with OSHA reporting requirements.
- The provision of data to health oversight agencies for the purposes of audits and investigations.
- For law enforcement purposes (subject to specified conditions).
- The disclosure of PHI to funeral directors, coroners, and medical examiners.
- To facilitate the donation and transplantation of organs, eyes, and tissue.
- To facilitate research (subject to specified conditions).
- When there is a serious threat to public health and safety.
- For workers’ compensation processes.
- To conduct essential government functions such as determining the suitability of an individual for a role within a U.S. State Department.

As well as having specific conditions attached to them, many of the allowable uses and disclosures of PHI are subject to specific processes. It is advisable for Covered Entities and Business Associates unfamiliar with these processes to seek professional HIPAA compliance advice.

**DISCLAIMER**

This PHI checklist is provided for information purposes only and does not qualify as legal advice. Understanding the HIPAA PHI definition, what is considered PHI under HIPAA, and when it is allowable to disclose PHI without patient authorization does not guarantee that you or your organization are HIPAA compliant. You should always consult a HIPAA compliance expert.