What is Considered PHI Under HIPAA Rules?

Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.

It is not only past and current health information that is considered PHI under HIPAA Rules, but also future information about medical conditions or physical and mental health related to the provision of care or payment for care. PHI is health information in any form, including physical records, electronic records, or spoken information.

Therefore, PHI includes health records, health histories, lab test results, and medical bills. Essentially, all health information is considered PHI when it includes individual identifiers. Demographic information is also considered PHI under HIPAA Rules, as are many common identifiers such as patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, when they are linked with health information.

The 18 identifiers that make health information PHI are:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any unique identifying number or code

One or more of these identifiers turns health information into PHI, and PHI HIPAA Privacy Rule restrictions will then apply which limit uses and disclosures of the information. HIPAA covered entities and their business associates will also need to ensure appropriate technical, physical, and administrative safeguards are implemented to ensure the confidentiality, integrity, and availability of PHI as stipulated in the HIPAA Security Rule.

When is PHI not PHI?

There is a common misconception that all health information is considered PHI under HIPAA, but there are some exceptions.

First, it depends who records the information. A good example would be health trackers – either physical devices worn on the body or apps on mobile phones. These devices can record health information such as heart rate or blood pressure, which would be considered PHI under HIPAA Rules if the information was recorded by a healthcare provider or was used by a health plan.

However, HIPAA only applies to HIPAA-covered entities and their business associates, so if the device manufacturer or app developer has not been contracted by a HIPAA -covered entity or a business associate, the information recorded would not be considered PHI under HIPAA.

The same applies to education or employment records. A hospital may hold data on its employees, which can include some health information – allergies or blood type for instance – but HIPAA does not apply to employment records, and neither education records.

Under HIPAA, PHI ceases to be PHI if it is stripped of all identifiers that can tie the information to an individual. If the above identifiers are removed the health information is referred to as de-identified PHI. For de-identified PHI, HIPAA Rules no longer apply.

When do I need a BAA?

A BAA (Business Associate Agreement) is required if you are going to share or enter any of the above PHI identifiers into a system/website/server not owned by the University of Utah.