# Identifying Protected Health Information (PHI)

PHI is at the very core of the Health Insurance Portability and Accountability Act (HIPAA). The underlying purpose of HIPAA is to keep personally identifiable information in a patient's health record or any information about his/her health private and protected. This includes **all** health information, whether physical, electronic, or verbal. To be considered PHI that is regulated under HIPAA, the information must meet two criteria:


1. Personally, identifiable to the patient
2. Used by or disclosed to/by a covered entity before, during, or after the course of care

The HHS defines **Protected Health Information** as all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI).

**Individually identifiable health information** is information, **including demographic data**, that relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and
- that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). If any of this information has been de-identified, meaning stripped of all individually identifiable health information, it is no longer considered PHI.

| The HIPAA Identifiers | |
|---|---|
| Name | Health plan beneficiary number |
| Address (all geographic subdivisions smaller than state; include street address, city, county, and zip code) | Account numbers |
| Dates (all elements of dates (except years) related to an individual); dates of birth, admission, discharge, death | Certificate or license number |
| Telephone number | Vehicle identifiers including license plates |
| Fax number | Web URL |
| Email address | Internet Protocol (IP) Address |
| Social Security Number | Finger or voice print (biometric identifiers) |
| Medical record number | Photograph - not limited to face images. |
| Any other characteristic that could uniquely identify the individual* | Device identifiers and serial numbers |

*Protected health information excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and employment records held by a covered entity in its role as employer.

Protected health information in electronic form is referred to as **ePHI**. This is simply the information described above delivered in an electronic format. The HIPAA Security Rule outlines the parameters for protection of this information in electronic form. Examples of ePHI that you may encounter in your office include but are not limited to:

| | |
|---|---|
| Authorization or Referral | X-rays, MRIs, CT scan reports, or images |
| Patient diagnosis on a form | Patient electronic health record |
| Emails from the patient or to the patient | Text message from patient or to the patient |
| Practice Management schedule for patient appointments | Demographic information in online intake form or patient request for information |

**Note:** In some states, there are laws regarding Individually Identifiable Health Information that are even more stringent than HIPAA. If you practice in one of these states, you need to consider these and create policies and procedures around these standards.