An external web page:

(<https://www.accountablehq.com/post/the-18-phi-identifiers>) (<https://www.healthitanswers.net/phi-or-pii-whats-the-difference/>)

(<https://www.hipaajournal.com/hipaa-privacy-rule/>)

(<https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis#:~:text=The%20HIPAA%20Security%20Rule%20requires,and%20security%20of%20this%20information>.)

**18 PHI Identifiers**

1. Name
2. Address
3. Dates
4. Telephone
5. Fax Number
6. Email Address
7. Social Security Number
8. Medical Record Number
9. Health plan beneficiary number
10. Account numbers
11. Certificate/license number
12. Vehicle identifiers, serial numbers, license plate numbers
13. Device identifiers/serial numbers
14. Web URLs
15. IP Address
16. Biometric identifiers – fingerprints or voiceprints
17. Full-face photos
18. Any other unique identifying numbers, characteristics, or codes.

**Difference between PHI and PII**

**PII** - Any information that can be traced to a person’s identity.

**PHI** – HIPPA-covered entities that contain identifiable health information

**Data elements that constitute data classification for HIPPA**

* Medical records
* Lab reports
* Hospital bills
* Mental Health assessments
* MRN, health insurance information

**HIPPA info location on Sharepoint**

* <https://central.nyumc.org/shared/legal/compliance/Pages/hipaa.aspx>

**HIPPA Privacy Rule**

The HIPAA Privacy Rule was first published in 2002 with the goal of protecting the confidentiality of patients and their healthcare information while enabling the flow of patient healthcare information when it is needed. (Governs use of all PHI, patient’s rights)

**Protected Information**

PHI is often accessed by insurance providers and clearing houses for billing information, individually identifiable health information not only includes such items as names, addresses, date of birth, and Social Security numbers, but also credit card information, vehicle registration plate numbers, and even electronically-stored examples of a patient´s handwriting.

**HIPPA Security Rule/Risk Analysis**

The HIPAA Security Rule requires physicians to protect patients' electronically stored, protected health information (known as “ePHI”) by using appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of this information.

**Safeguards:**

1. **Administrative** - HIPAA defines administrative safeguards as, “Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.” (45 C.F.R. § 164.304).
2. **Physical** - safeguards involve access both to the physical structures of a covered entity and its electronic equipment (45 CFR §164.310). ePHI and the computer systems in which it resides must be protected from unauthorized access, in accordance with defined policies and procedures.
3. **Technical** - Technical safeguards encompass the technology, as well as the policies and procedures for its use, that protect ePHI and control access to it. They are often the most difficult regulations to comprehend and implement (45 CFR §164.312).

**Risk Assessment**

To comply with the Security Rule’s implementation specifications, covered entities are required to conduct a risk assessment to determine the threats or hazards to the security of ePHI and implement measures to protect against these threats and such uses and disclosures of information that are not permitted by the Privacy Rule.