# Protected Health Information (PHI)

## What is Protected Health Information?

The HIPAA Privacy Rule protects most "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. The Privacy Rule calls this information *protected health information*:

1. That identifies the individual; or
2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual is protected.


To support patient care, providers store electronic Protected Health Information (PHI) in a variety of electronic systems, not just Electronic Health Records (EHRs). Knowing this, providers must remember that all electronic systems are vulnerable to cyber-attacks and must consider in their security efforts all of their systems and technologies that maintain PHI.

## Nemsys Security Measures:

- DATA Encryption: at rest and in transit
- Actively monitored endpoint threat management
- Automated offsite data backup for system recovery
- Unique user IDs and strong passwords
- Frequent password refresh policy
- Role- or user-based access controls
- Auto time-out with screen lock
- Extensive log and access auditing
- Business continuity documentation
- Email security and encryption
- Secure remote access
- Web filtering, monitoring and tracking
- Mobile security management
- Advanced network security gateway
- Compliance testing and auditing

The following identifiers of the individual or of relatives, employers, or household members of the individual, are considered PHI identifiers under HIPAA:

1. Names
2. Postal address All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the 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
   - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers
5. Fax numbers
6. Electronic mail address
7. Social security numbers
8. Medical record numbers
9. Account numbers
10. Health plan beneficiary number
11. Certification/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Name of relative
15. Web Universal Resource Locator (URL)
16. Internet Protocol (IP) address number
17. Biometric identifiers, including fingers and voice prints
18. Full face photographic images and any comparable images
19. Any other unique identifying number, characteristic, or code

# Protected Health Information (PHI)

connect powered by nemsys

## Keeping PHI Secure with Nemsys

The Security Rule has several types of safeguards and requirements which you must apply:

1. ***Administrative Safeguards*** – Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of workforce members in relation to the protection of that information. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to PHI and then implement security measures to reduce the identified risks.

2. ***Physical Safeguards*** – These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. These safeguards are the technology and the policies and procedures for its use that protect PHI and control access to it.

3. ***Organizational Standards*** – These standards require a CE to have contracts or other arrangements with BAs that will have access to the CE's PHI. The standards provide the specific criteria required for written contracts or other arrangements.

4. ***Policies and Procedures*** – These standards require a CE to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A CE must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments. A CE must periodically review and update its documentation in response to environmental or organizational changes that affect the security of PHI.

## Encryption 101

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (a type of formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

## Cybersecurity

Cybersecurity refers to ways to prevent, detect, and respond to attacks against or unauthorized access against a computer system and its information. Cybersecurity protects your information or any form of digital asset stored in your computer or in any digital memory device.

It is important to have strong cybersecurity practices in place to protect patient information, organizational assets, your practice operations, and your personnel, and of course to comply with the HIPAA Security Rule. Cybersecurity is needed whether you have your EHR locally installed in your office or access it over the Internet from a cloud service provider.