**EXPLANATION AND DEFINITION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) OR PROTECTED HEALTH INFORMATION (PHI)**

**Definition of PII as relates to Cyber Insurance**

The definition of PII is personally identifiable information. This is information that, on its own or combined, can be used to identify, locate, or contact an individual. Some examples of PII are obviously sensitive: Social Security number, credit card number, driver’s license number, and account numbers. Others are less obvious but just as important: full name, date of birth, home address, phone number, employment history, purchase history, email address, or even a photo of an individual’s face.

**Definition of PHI as relates to Cyber Insurance**

The definition of PHI is protected health information. It is a subset of PII that is protected by the [HIPAA Privacy Act of 1996](https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html). PHI is information that can be used to identify an individual AND that relates to that individual's past, present, or future physical or mental health care or health care payments. Some examples of PHI are: any and all PII gathered in the course of providing health services, medical, dental, or prescription drug records, insurance coverage, health plan number, status in a government health program, and dates of hospitalization.

**Cybersecurity best practices**

Start out with the fundamentals (this is not an exhaustive list):

* Use a firewall.
* Use good password policies.
* Antimalware software that is automatically updated.
* Have policies addressing allowable software and internet usage.
* Have policies addressing the business use of personal devices.
* Keep servers and workstations continuously patched.
* Perform regular system backups.
* Monitor system logs and security alerts.
* In addition to these, when dealing with PHI, it is especially important to use encryption in all its forms:
* A remote-access VPN for mobile users to establish secure connections with your network.
* Encrypted email messages to protect content from being read by someone other than the intended recipients.
* Encryption at rest to secure data persistently stored on any mobile device including laptops, tablets, and phones.
* Endpoint encryption to secure data that is copied to USB flash drives or memory cards.

Because cybercriminals use eyes, ears, and phones almost as much as they use computers, do the following  (this is not an exhaustive list):

* Locking screen savers should be activated on computers accessing PHI.
* Computer screens should be positioned so that only the user can see the screen (beware of windows behind you).
* Minimize paper usage. “Instead of writing on a post it, use a whiteboard and erase it.”
* Printers and FAX machines used for PHI must be placed in private areas.
* Documents should be picked up immediately and disposed of in shred bins when finished.
* Implement a clean desk policy. No PHI should be unlocked when a person is away from their work area.
* PHI must never be removed from the office unless there is a clear business need.
* Never leave any mobile device containing PHI unattended or out of reach.
* Don’t discuss PHI in public areas.

Information is one of our most precious resources and is the asset that powers and enables our business. Let’s treat it that way.