HIPAA Privacy & Your EMR:
Meet the Requirements to Protect the Patient & Your Business

The HIPAA Privacy rule simply put is a construct to enforce industry guidelines that help prevent unauthorized access to PHI (Protected Health Information). Regarding PII (Personally Identifiable Information), the rule establishes standards on removing identifiers from healthcare data, known as de-identification (45 CFR §164.514(a)-(b))[i]. The rule covers many aspects of healthcare provider practices within these categories:

Use & Disclosure	Administrative Safeguards	Patient Access	Data Security	Breach Reporting

In terms of IT Security, the primary source of guidelines is the National Institute of Standards and Technology (NIST). The rapid transition from paper-based patient records to an EMR (Electronic Medical Record) system has increased the awareness of cyber threats and the importance to adhere to security guidelines defined by the privacy rule, NIST, FCC, and others.

Compliance ownership falls primarily on the healthcare provider itself. It is important when choosing an EMR software vendor to understand the mechanisms built into the product to safeguard sensitive information. Two common methods used by EMR software vendors to assist in this effort are *data encryption and masking the associations of data elements* to prevent the linking of information to an individual.

As a provider, the first step toward cyber security compliance is ***Risk Analysis***. This process should identify areas of vulnerability and establish a plan to employ practices that prevent or mitigate the threat of a data breach. The general areas to be investigated include:

Network Design	Patch Management	User Education	Business Continuity

Network Design refers to the communication infrastructure of any computer environment. The design must maintain the flow of data and enforce access rules to ensure information is limited to only allowed destinations. Proper network design is the primary defense against cyber threats within an organization.

All software applications have vulnerabilities. As these are discovered, software vendors address the risks by releasing security patches. A well-implemented **Patch Management** process should include computer operating system, anti-virus protection packages, and network equipment updates. In many cyber-attack instances, organizations fall victim to a known exploit for which a security patch has already been released.

Staff members who interact with your EMR system will often be the first to notice irregularities on their computers. For this reason, continued security awareness training for end-users is crucial to the safeguarding of patient data. Areas of **User Education** should, at a minimum, focus on email, web browsing and general tips to identify potentially malicious activity. Training of this nature is recommended on a semi-annual basis with the distribution of monthly updates. From a compliance perspective, proof of participation in this training is required.

When data has been rendered inaccessible due to a cyber-attack, your ability to recover determines your susceptibility. A well-implemented **Business Continuity** plan is the final defense against an exploit. Data protection elements of the plan should range from local file restoration to disaster recovery procedures. Defining your *Recovery Time* and *Recovery Point Objectives* are other key components of the plan to ensure failover requirements are met. Inadequate and untested recovery procedures can be fatal to a healthcare organization.

When thinking in terms of Emergency Preparedness, understand the data security risks within your environment that can impede your ability to provide care. The guidelines set forth in the HIPAA Privacy Rule are designed to help mitigate these risks and ultimately protect the patient and your business.

---

[i] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale

Provided in Collaboration with Innovative Business Technologies

Simione™ HEALTHCARE CONSULTANTS

Learn more and get help at 844.215.8820 **Simione.com**