CYBER SECURITY Newsletter

HIPAA

Problem

Medical science has made tremendous advances in the past twenty years, from new medicines and surgery techniques to decoding the human genome. With this wealth of new knowledge has come a better understanding of how to improve the general health of people.

However, with all these advances comes a new challenge: what to do with the information that is recorded for each patient -- information such as patient's medical conditions, their treatment plans, and how they pay for their medical services. All of this confidential personal information must be protected. While at the same time, to effectively treat patients, this information may need to be shared with a variety of doctors, nurses, lab technicians, and accounting personnel throughout different organizations.

Solution

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPPA). One of the requirements of HIPAA is the protection of Protected Health Information, known as PHI. PHI is the formal name given to any individually identifiable health information, such as a person's medical records or health care payments.

As our organization handles PHI, we are required by HIPPA to adhere to specific rules on handling it. This newsletter explains what PHI is and the rules we must follow to protect it. These rules apply to PHI in digital, oral, and written formats.

Protecting Patient Data

Since our organization handles patient data, we need to understand and follow the security regulations known as HIPAA. This newsletter explains what those standards are and how to follow them.

Idaho State University

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

Examples of Patient Data

Patient related information, or PHI, can be made up of a variety of different types of data. First, the information has to be identifiable to a specific individual, such as a patient's name or social security number. Second, not only can the medical information be anything related to medical diagnosis or treatment, but also any payment-related matters, such as costs of treatment.

Below is an example of PHI. Remember the rules of HIPAA and how PHI is handled does not only apply to digital information, but any PHI in oral or written form.

EXAMPLE PHI
Name: John A. Smith
Date of Birth: April 15, 1987
SSN: 078-05-1120
Address: 1060 W. Addison, Chicago, IL 60613
Diagnosis: Prostrate Cancer
Treatment: Chemotherapy
Payment Due: $23,456

1. Authorized Personnel
Only share patient data with authorized personnel. You must obtain the patient's written authorization for any use or disclosure of PHI that is not for direct care or treatment.

2. Minimum Necessary
A central aspect of HIPAA is the principle of "minimum necessary" use and disclosure. You must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

3. Authorized Systems
Use only authorized systems to enter, process, or store protected health information. Do not copy or store PHI to any unauthorized systems.

4. Health Care Use
Do not use PHI systems for non-work related or unauthorized activities, such as surfing the web, reading personal email, or chatting with someone online. Activities such as these can expose patient data to great risk.

5. Transferring Health Care Data
Transfer of protected health information must use secure, authorized methods, including the use of encryption. Do not transfer PHI using insecure means such as FTP or email unless sensitive data has first been encrypted.

6. Disposing of PHI
All physical and electronic PHI that is no longer necessary or appropriate to store must be properly destroyed, shredded, or rendered unreadable.

7. Lost or Stolen PHI
If you believe any PHI has been accidently lost or stolen, please report the incident right away. The sooner our organization is aware of the problem, the quicker we can react and protect the patient data.