CYBER SECURITY newsletter

HIPAA

Problem

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

However, with all of these advances comes a new challenge, what to do with all the information that is recorded for each patient. Information such as patient medical conditions, their treatments and how they will pay for these medical services. All of this highly personal information has to be protected. However, at the same time to effectively treat patients, this confidential information has to be shared with a variety of people in different organizations, including doctors, nurses, lab technicians and accounting.

Solution

In 1996 U.S. Congress enacted HIPAA, or the Health Insurance Portability and Accountability Act. 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 HIPAA to adhere to specific rules on handling it. This newsletter explains what PHI is and the seven rules we must follow to protect it. In addition, these rules apply not only to PHI in digital format, but any other format, including oral and written.

Protecting Patient Data

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

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

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. Below is one example of what PHI can look like. Remember, the rules of HIPAA and how PHI is handled does not just apply to digital information, but any PHI in oral or written form also.

EXAMPLE PHI
Name: John A. Smith
Birth date: 15 April 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 who have a need to know. You must obtain the individual'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, to include 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. Finally, 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 better we can react and protect the patient data.