HIPAA PRIVACY AND SECURITY AWARENESS

Introduction

The Health Insurance Portability and Accountability Act (known as HIPAA) was enacted by Congress in 1996. HIPAA serves three main purposes:

› To protect people from losing their health insurance if they change jobs or have pre-existing health conditions.

› To reduce the costs and administrative burdens of healthcare by creating standard electronic formats for many administrative transactions that were previously carried out on paper.

› To develop standards and requirements to protect the privacy and security of personal health information.

Introduction

Entities covered by the Privacy and Security Rules include:

› Healthcare plans

› Healthcare providers

› Healthcare clearinghouses

› Business associates of covered entities, which include auditors, consultants, lawyers, data and billing firms and others with whom the covered entities have agreements involving the use of protected health information.

Protected Health Information

No matter what form it takes, notes on a medical chart, health information entered into a computer or discussions about a patient's condition, any identifiable health information becomes protected health information (PHI) under HIPAA.

A covered entity may not use or disclose protected health information except:

› As the individual authorizes in writing; or

› As the HIPAA Privacy Rule permits or requires.

Protected Health Information

PHI can be disclosed:

› To the individual or their authorized representative.

› For treatment, payment or healthcare operations.

› When the individual has the opportunity to agree or object, such as when the patient brings another person into the exam room for their office visit.

› Incidental to an otherwise permitted use.

› For the purposes of research or public health.

Professional ethics and good judgment should also be relied upon in deciding which of these permissive uses and disclosures to make.

Protected Health Information

Covered entities are required to provide patients with a Notice of Privacy Practices and make a good faith effort to obtain a patient's written acknowledgment of receiving the notice.

The notice must inform patients of (1) the uses and disclosures of PHI that may be made, (2) the patient's right to access and amend their medical information, and (3) the covered entity's responsibilities with respect to PHI.

The entity may use PHI for its own treatment, payment or healthcare operations and may disclose PHI to other covered entities. Reasonable efforts to limit PHI to the minimum necessary should be taken when using or requesting PHI.

Patient Access

Except in certain circumstances, individuals have the right to review and obtain copies of their protected health information. Personal representatives, parents
of minors and others may also be legally authorized
to make healthcare decisions on behalf of patients. Covered entities may impose reasonable, cost-based fees (postage and cost of copying) for PHI request.

Other Uses of PHI

As a general rule, covered entities may not use or disclose PHI for any purpose other than treatment, payment and healthcare operations without the patient's written authorization. The Privacy Rule does allow for "incidental" disclosure of PHI as long as the covered entity used reasonable safeguards and adheres to the "minimum necessary" standard. For example, the use of waiting room sign-in sheets would be considered "incidental" disclosure of PHI.

Administrative Safeguards

Since many employees receive, store and transmit PHI as part of their daily routine, the Privacy Rule requires the following safeguards:

› A Privacy Officer must be designated for the purpose of developing and implementing privacy policies and the receiving of complaints.

› All workforce members must be trained on privacy policies and procedures.

Administrative Safeguards

› Requires all business associates must confirm that they will protect PHI.

› A system must be developed to track who accessed what information.

› Rules must be implemented for addressing violations of privacy, security and transaction regulations, and establish a process for making complaints and preventing retaliation against anyone who reports
a HIPAA violation.

Safeguards for Security

Administrative Safeguards

Requirements include:

› Designating a Security Officer in charge of developing, implementing and evaluating security policies. This may be the same person as the
Privacy Officer.

› Ensuring computers are secure from intrusion.

› Applying appropriate sanctions against employees who fail to comply with HIPAA policies.

Safeguards for Security

› Implementing procedures to regularly review records of information system activity.

› Developing a plan for granting and limiting different levels of access to PHI, including clearance and termination procedures. This includes security checks and special training for all employees with access to sensitive information.

› Providing a contingency plan for responding to system emergencies.

› Implementing procedures for reporting and dealing with security breaches.

Safeguards for Security

Physical Safeguards

The Security Rule also requires a number of physical steps to ensure that PHI contained in computers is protected. A facility security plan should be developed that deters intruders from accessing areas where PHI resides. Guidelines should be established on how to handle sensitive information that may be displayed on computer screens. The safeguarding of information on hardware and software must also be utilized, as well as, procedures for off-site data backup.

Safeguards for Security

Technical Safeguards

The Security Rule requires certain technical safeguards for PHI.

› Controls to ensure that access to sensitive information is available on a need-to-know basis must be established.

› Audit controls to record and examine system activity.

› Controls to help ensure that health data has not been altered in an unauthorized manner.

Safeguards for Security

› Controls to ensure that data is sent to the intended recipient and received by the intended party (including the use of passwords, PIN numbers and encryption).

› Controls to protect PHI sent via e-mail and fax. According to the Security Rule, it is permissible to use the internet to transmit PHI. An acceptable method of encryption must be used and appropriate authentication procedures followed to ensure correct identification of the sender and receiver. Faxes are not considered to be “covered transactions” by the Security Rule. They may be sent as authorized by your company’s privacy policy.

Compliance and Enforcement

The HIPAA regulations are now completely in effect and failure to comply with the HIPAA Privacy or Security Rules can lead to significant financial and other penalties. Civil and criminal penalties, to both individuals and companies, may be enforced and include fines up to $1.5 million and ten years of imprisonment. It is important that all who may come into contact with PHI understand and carry out their responsibilities under these rules, as outlined in this training program.