HIPAA Privacy Requirements

Policy

The Claims Research and Resolution Department will take reasonable steps to ensure that all Protected Health Information (PHI) is handled in a manner that protects the privacy and security of the information and prevents that information from misuse and unauthorized access.

As required by law, the Claims Research and Resolution department will implement procedures to ensure that all PHI is accessed only when needed to process payment for those services and additionally that specific procedures are in place to ensure that PHI is not inadvertently shared or made available outside of those requirements.

This policy addresses the following requirements:

- Procedures for email transmission of PHI
- Procedures for discussion of PHI in conversations
- Procedures for the use of PHI in training material
- Procedures for security of PHI on printers and faxes
- Procedures for security of PHI within the workspace
- Procedures for Information taken out of the workplace for business purposes

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates that all covered entities must make reasonable attempts to protect and secure all identifiable health information. This includes Protected Health Information (PHI) maintained or communicated on paper, electronically or orally.

Definitions

PHI is defined as any information about an individual that relates to the individual's:

- Past, present or future physical or mental condition
- Provision of health care services
- Payment for the provision of health care services

There are two components regarding PHI. The first component refers to any information that allows for identification of an individual. The second component refers to information regarding their health information.

Continued on next page

HIPAA Privacy Requirements, Continued

Types of PHI

PHI includes, but is not limited to, the following identifying information:

- Name
- Date of birth
- Address
- Social Security Number
- Telephone number
- Email Address

PHI also includes, but is not limited to, the following health information:

- Provider
- Diagnosis
- Date of service
- Type of service

Employee Responsibility

Because the Claims Research and Resolution Department works to ensure the timely and correct payment of claims for medical services, department employees are authorized to utilize PHI in their day to day duties.

Each employee is responsible for following the company policies and procedures to ensure that PHI is disclosed only when appropriate and necessary according to the requirements of the law and that appropriate security measures are maintained when disclosing this information.

Appropriate Disclosure

PHI can only be accessed or shared when it is necessary for medical treatment and payment for those services.

Additionally, all healthcare providers must ensure that specific policies are in place to maintain the privacy and security of PHI for any reason that is not required for medical treatment and payment for those services.

Continued on next page

HIPAA Privacy Requirements, Continued

Consequences of violations

If an employee is found to be in violation of this policy, the following actions will be taken:

Offense	Action
First offense	Verbal warning and training
Second offense	Written warning
Third offense	Probation or termination

Procedures for Specific Situations

Procedures will be implemented to maintain the security and integrity of PHI in the following situations:

- Procedures for transmission of PHI in email communication
- Procedures for discussion of PHI in conversations
- Procedures for the use of PHI in training material
- Procedures for security of PHI on printers and faxes
- Procedures for security of PHI within the workspace
- Information taken out of the workplace for business purposes

Email Transmission

PHI must be sufficiently protected during the transmission of electronic communication.

Password protection of a file that includes PHI is not adequate to protect the security of the information. All email communication containing PHI must be encrypted to ensure the security of the information.

The IT department has initiated a procedure to ensure that external electronic communication is properly safeguarded. When sending an email that includes PHI, the subject line of the email communication must include the word “PHI”.

Electronic security systems have been updated to scan the subject line and encrypt the data included in that transmission. Attachments that include PHI are also encrypted and password protection for attachments is not necessary.

Additionally, email communication from outside sources that has not been encrypted cannot be accepted. A password protected file is not sufficient to meet the security requirements.

When files with PHI need to be transmitted to or from an external partner, it is best to utilize a cloud service.

Continued on next page

Procedures for Specific Situations, Continued

Conversation	It is important that each employee be aware of their surroundings when discussing PHI for business purposes. Employees should be confident that the conversation cannot be overheard by people who are not authorized to access the information. Conversation regarding PHI should not take place in public spaces.
Training Material	When member information is used to create scenarios in training material, all efforts must be made to protect identifying information to prevent the accidental release of confidential information and to protect the member from identity theft. Information that is not necessary for the scenario should be blacked out or removed from the material. Additionally, training material that contains PHI must be safeguarded in the same manner as any other printed or electronic document.
Printers and Faxes	Employees must make all possible efforts to ensure that documents containing PHI are not left on printers and faxes for extended periods. Printers and faxes should be checked prior to the close of business to ensure that documents containing PHI are not left unsecured.
Workspace	Each employee is responsible for ensuring that PHI is secured when they are away from their workspace. When leaving the workspace for a period of time over 5 minutes, such as breaks, lunches and meetings, the computer should be locked and documents containing PHI should be covered so that the information is not visible. When leaving the workspace at the end of the day, the computer must be locked and all documents containing PHI must be locked in a drawer or cabinet.

Continued on next page

Procedures for Specific Situations, Continued

Information Taken Outside of the Office	At times, the employee's job function may require that documents containing PHI are taken out of the office. When this occurs, the employee is responsible for ensuring the security of the information by keeping it locked in a case or retain it in the employee's possession.
Individual Responsibility	Each employee is responsible for executing all procedures as necessary. When all procedures are followed, the company can be confident that all reasonable efforts are being made to protect the PHI and adhere to the regulatory requirements. If an employee becomes aware that the policy is not being followed and that PHI is vulnerable, that employee has a responsibility to report the information to protect both the member and the company.