NIGHTINGALE
HIPAA AND PHI INSERVICE

Timely, accurate and complete health information must be collected, maintained and made available to members of the team so that members of the team can accurately diagnose and care for that individual. Most consumers understand and have no objections to this use of their information.

On the other hand, consumers may not be aware of the fact that their health information may also be used as:

- a legal document describing the care rendered
- verification of services for which the individual or a third-party payer is billed
- a tool in evaluating the adequacy and appropriateness of care
- a tool in educating heath professionals
- a source of data for research
- a source of information for tracking disease so that public health officials can manage and improve the health of the nation
- a source of data for facility planning and marketing

Although consumers trust their caregivers to maintain the privacy of their health information, they are often skeptical about the security of their information when it is placed on computers or disclosed to others. Increasingly, consumers want to be informed about what information is collected, and to have some control over how their information is used.

With this in mind, some states and more recently, the federal government passed legislation requiring that health plans, healthcare clearinghouses; and healthcare providers furnish individuals with a notice of information practices.

Furthermore, a covered entity must provide a notice to patient that they may not use or disclose protected health information in a manner inconsistent with such notice, referred to Notice of Privacy Practices.

Overview of HIPAA Regulations[1]

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), one purpose of HIPAA is to protect health information by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information, HIPAA applies to health plans, health care clearing houses and health care providers.

The administrative simplification provision of HIPAA has three major requirements:

- Protection for the privacy of Protected Health Information
- Protection for the security of Protected Health Information
- Standardization of electronic data interchange in health care transactions

[1] www.mmcc-tlc.com

Any information that can identify a patient is called Protected Health Information (PHI). This information can be spoken, written or in a computer. Some examples might be the person's name, address and phone number, but also includes things such as the person's credit card number, email address or family member's names. Employees are not permitted to email or text information about patients via personal emails or phones.

An individual's permission is needed to use or disclose protected health information for specific purposes other than to carry out treatment, payment of health care operations is required.

Patients have the right to request a restriction of the use or disclosure of their health information.

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose or the use, disclosure or request.

Health care agencies will not release a patient's entire medical record unless the release of the whole record is justified as reasonably necessary to accomplish the purpose of the requested use or disclosure.

Individual Rights
The privacy rule creates five individual rights. Covered entities must furnish patients the following information about their rights.

1. Right to notice of the covered entity privacy practices.
2. Right to request restrictions and confidential communications concerning protected health information.
3. Right to obtain access to protected health information for inspection and copying.
4. Right to obtain an accounting of certain disclosures.
5. Right to request amendment of protected health information.

Although consumers trust their caregivers to maintain the privacy of their health information, that may be made by the covered entity, as well as the individual's rights, and the covered entity's legal duties with respect to protected health information.

Identity Theft
It is the policy of Nightingale to develop, implement and maintain a comprehensive Identity Theft Program to detect, prevent and mitigate identity theft in connection with the openings of all covered patient accounts or any existing covered patient accounts. This policy and subsequent procedures are designed to control reasonably foreseeable risks to customers and to ensure the safety and soundness of the institution from identity theft.

Identity theft occurs when fraud is committed or attempted using the identifying information of another person without authority. Identifying information means "any name or number that

may be used, alone or in conjunction with any other information to identify a specific person including:

- Name, social security number, date of birth, official State of government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation;
- Unique electronic identification number, address or routing code; or
- Telecommunication identifying information or access device. "Access Device" means: Any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number or other telecommunications service, equipment or instrument, alone or in conjunction with another access device, to obtain money, goods, services or any other thing of value or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instruments).

Therefore, identity theft includes not only a thief opening an account in someone else's name, it also includes unauthorized use of account or access device numbers (such as credit card and debit card numbers), access devices passwords for online access or other means to access an account.

Medical Identity Theft
Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity –such as insurance information – without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

Some examples of identity theft include:

- Stealing mail, such as intercepting billing services, bank or other financial statements;
- Diverting mail from its intended addressee by submitting a forged change of address request;
- Impersonating a patient or a patient's relative, guardian, or person entitled to receive patient information or impersonating a employee of the institution or someone entitled to receive information about an employee in person in order to obtain information from institution, banks and other businesses;
- Intercepting or otherwise obtaining information transmitted electronically;
- Rummaging through trash for personal data;
- Stealing wallets that contain personal identification information and credit cards; or
- Stealing personal identification information from patient or workplace records.

A customer affected by identity theft may not realize that someone has stolen their identity for months or even years. The victim may only realize this has happened once they are denied credit or until a creditor attempts to collect on an unpaid bill.

A business entity that has engaged in virtually any commercial transaction with a person *(including extending credit or selling goods or services)* who has allegedly made unauthorized use of the means of identification of the victim *(an identity thief)* must provide certain required information to victim not later than 30 days after receipt of a request from a victim.

RED FLAGS

The following subtopics represent categories of "red flags" that are used by our institution within its Identity Theft Program to help detect identity theft in connection with the openings of accounts and existing accounts by:

1. Obtaining identifying information about and verifying the identity of, a person establishing an account or attempting to gain information about an account.
2. Authenticating customers, monitoring transactions and verifying the validity of change of address requests or change of health care power of attorney appointees with existing accounts.

These categories and detection techniques ("Red Flags") are designed to prevent and mitigate the risk of identity theft;

Presentation of Suspicious Documents:

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer (such as, the patient) presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the institution.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Presentation of Suspicious Personal Identifying Information

1. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
2. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third party sources used by the institution, such as;
    - The address on a document is the same as the address provided on a fraudulent document; or
    - The phone number on a document is the same as the number provided on a fraudulent document.

3. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third party sources used by the Institution, such as:
    - The address on a document is fictitious, a mail drop, or prison; or
    - The phone number is invalid, or is associated with a pager or answering service.
4. The SSN provided is the same as that submitted by other persons opening an account or other customers.
5. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
6. The person opening the account or the customer fails to provide all required personal identifying information on a document or in response to notification that the document is incomplete.
7. Personal identifying information provided is not consistent with personal identifying information that is on file with the Institution.

Unusual Use of, or Suspicious Activity Related to an Account

1. Shortly following the notice of a change of address for an account, the Institution received a request for new or additional authorized names on the account.
2. An account is used in a manner that is not consistent with established patterns of activity on the account, such as;
   * Nonpayment when there is no history of late or missed payments;
   * A material increase in the use of available credit; or
   * A material change in usage patterns such as treatment for a condition never observed before.
3. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
4. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
5. The Institution is notified that the customer is not receiving paper account statements.
6. The Institution is notified of unauthorized charges or transactions in connection with a customer's account.
7. The customer reports an inaccurate record.

Other Notices Regarding Possible Identity Theft

Such notices can be from customers, victims of identity theft, law enforcement authorities, or other persons notifying the Institution that it has opened a fraudulent account for a person engaged in identity theft. It is the policy of the institution and the responsibility of all personnel to appropriately respond to events of suspected or identified cases of identity theft and red flags that are commensurate with the degree of risk posed. In determining an appropriate response, the Institution has considered aggravating factors that may heighten the risk of identity theft, such as:

1. A data security incident that results in unauthorized access to a customer's account records held by the Institution or third party; or
2. Notice that a customer has provided information related to an account held by the Institution to someone fraudulently claiming to represent the Institution or to a fraudulent website

In the event proof of positive identity of the victim (actual patient) is made, Company personnel should notify their supervisor immediately for immediate investigation. The Company will notify each affected state resident, and, if required due to number of individuals affected, notify local authorities and the Consumer Protection Division of the Department of Consumer Affairs and certain consumer reporting agencies.

Furthermore, the Fair Credit Report Act (FCRA) spells our rights of victims of identity theft, as well as responsibilities for businesses. The Federal Trade Commission (FTC) enforces the FCRA including this requirement, which is known as Section 609(e). The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices and to provide information to help consumers spot, stop, and avoid them. To get free information or to file a complaint on consumers issues, visit ftc.gov or call toll-free 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.[2]

To learn more about privacy issues and how they affect your life and the decisions you may make visit ftc.gov/privacy.

[2] Referenced from the Federal Trade Commission, Bureau of Consumer Protection, ftc.gov/privacy