VIDANT HEALTH

HIPAA Training for the Observation Experience

What is HIPAA?
The Health Insurance Portability and Accountability Act (HIPAA) establishes federal government standards and requirements for maintaining and transmitting health information. It defines Protected Health Information (PHI) and protects this information (i.e. name, phone number, Social Security Number (SSN), Medical Record (MR) number, addresses of residence (include street number, city, zip code), account numbers, and other criteria that identifies a patient. Every employee should know what information is protected.

What does HIPAA do?
Requires health care providers and health plans to maintain administrative, physical, and technical safeguards to protect confidentiality of, and prevent unauthorized access to, health information.

HIPAA has four components we must comply with:

- Privacy
- Transactions and Code Sets
- Security
- Unique identifiers

Who does HIPAA apply to?
Health care providers, health plans, and health care clearinghouses, and their business associates.

What are the requirements for compliance?

- Appoint a Privacy officer
- Appoint a Security officer
- Business Associate Contracts (if patient information is exchanged)
- Minimum necessary (only access to patient information to do your job)
- Notice of Privacy Practices (given to each patient upon admission)
- Patient authorizations (prior to release of information)
- Education around HIPAA requirements for anyone coming into contact with patient information
- Accounting for disclosures (so patients know who gets their information)
- Complaint process
- Administrative processes to manage security risk, incidents, access management and business continuity.
- Physical measures to protect security of facilities, equipment, and devices
- Technical measures to control access and protect information at rest and in motion
- Policies and procedures regarding privacy and security requirements
- Policies and procedures to respond to and report breaches in the confidentiality of confidential information
What happens if we are not in compliance?

Under significant revisions to HIPAA under the HITECH Act (Final rule 9/24/09) we must let patients know when their confidentiality has been breached. In some cases, we must also notify the federal Department of Health and Human Services, who will post the information on their website. If we are unable to contact the affected individuals, we may also be obligated to alert the news media and/or place a public notice on our website. Under state law, we must also notify the NC Attorney General’s Office.

In addition, HIPAA violations are now subject to tiered penalties based on whether or not the covered entity knew of the breach of privacy, and whether the breach was due to reasonable cause or willful neglect. The tiered penalties are as follows:

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknowing violation</td>
<td>$100 to $50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>Maximum $1,500,000 per type of violation per calendar year</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 to 50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>Maximum $1,500,000 per type of violation per calendar year</td>
</tr>
<tr>
<td>Willful neglect, corrected</td>
<td>$10,000 to $50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>Maximum $1,500,000 per type of violation per calendar year</td>
</tr>
<tr>
<td>Willful neglect, uncorrected</td>
<td>Minimum $50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>Maximum $1,500,000 per type of violation per calendar year</td>
</tr>
</tbody>
</table>

Important Note: both the covered entities and its employees/agents are subject to both civil and criminal penalties for HIPAA violations.

What does HIPAA mean to you?

We expect everyone to abide by the privacy and security policies and procedures. Failing to do so will result in disciplinary action up to and including termination from the shadowing experience.

The following is information that is important for all staff to use when making decisions about use of Protected Health Information (PHI)

**PHI** – Identifiers of the individual, or relatives, employers or household members of the individual. Identifiers include: name, all geographic subdivisions smaller than a state, all elements of dates relating to the individual, telephone numbers, and FAX numbers, E-Mail addresses, Social Security Number, medical record numbers, health plan beneficiary number, account numbers, certificate/license number,
vehicle ID’s, device identifiers and serial numbers, Web URL’s, IP address numbers, biometric indicators (including voice and fingerprints) and any other unique identifying number, characteristic, or code.

Minimum Necessary – A Covered Entity has an obligation to limit use, disclosure or request for PHI to the minimum necessary to accomplish the intended purpose. “If you don’t need it to do your job, then you should not be accessing or using it.”

Communication – Be mindful about communication in the community and in public places when you are discussing patient information. It is important that you keep PHI private. If you obtain information in the course of doing your job, it is NOT okay to share it without the patient’s permission unless it is related to treatment, payment or health care operations.

Computer Access – It is a privacy violation to look up information on the computer that you do not have a need to know to do your work. This includes information about you, or your family members. If you want access to your information, you must request access to the information through the Health Information Management Office (HIMS). Your sign-on is like your computer signature. It is used to identify you and to track your access to the computer system(s). Do not ever share your sign on or passwords with anyone. Avoid using passwords that can easily be guessed, i.e. family member names, pets, and friends. The computer is made available for you to do your work.

Misdirected FAX’s – If a FAX with PHI on it is sent to the wrong place or does not arrive at its intended destination, it is considered a critical event. This must be reported to Vidant Health Risk Management on call at (252) 413-4473, who will instruct you on how to respond.

Electronic Mail (E-mail) and Internet – E-mail and the Internet are the most widely used methods for spreading computer viruses and malicious software code. Use extreme caution when communicating or using these services. These services are owned by Vidant Health, and are the Organizations property. This gives Vidant Health the right to monitor any and all email and Internet traffic by users.

Leaving Documents Unsecured – Please make sure that ANY paper documents with PHI on them, goes into the Super Shred container when they need to be discarded. Leaving documents with PHI in unsecured locations can be a privacy violation and can cause serious harm to the patient if the information falls into the wrong hands.

Auditing – There is a process in place that includes auditing both our computer systems and the physical environment for potential privacy and security violations. If a violation is suspected, Vidant Health Risk Management initiates an investigation, in conjunction with the Privacy Officers. Auditing is done on a regular recurrent schedule, and violations reported to the appropriate management staff for action and follow-up.

Sanctions – The sanctions process is designed to assure consistent discipline for patient privacy and security violations. Sanctions are determined by the HR/VP Group. If allegations of privacy and/or security violations are substantiated, disciplinary action up to and including immediate termination is applied to the offenders.
Please help us safeguard patient information whether written, oral or electronic information.

1. Conversations about patients should not be conducted in public – avoid discussions around nursing stations, outside patient rooms, etc
2. Confidential information should not be exchanged via analog cell phone.
3. Never share your computer sign-on information.
4. Never discard any paper with patient information or labels with patient identifiers in the regular trash. Shred bins are located in numerous locations.
5. Never store confidential information on a portable device unless it is encrypted.

Help Vidant Health be HIPAA Right.

We need your continued help. With everyone focused on privacy and security of patient information, we can do our best to make sure that every patient’s information is held in the strictest confidence; and patients can be assured that we are respectful of their privacy.

For Privacy questions, contact the Vidant Health Privacy Officers at 847-1924

For IT Security questions, contact the IT Security Officer at 847-5155
HIPAA Training for the Observation Experience

What you need to know for HIPAA Compliance

HIPAA Policies and Procedures

Policy/Process: Reportable Privacy Breach

Critical Elements:

Breach

*Breach* means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of [45 CFR §164] which compromises the security or privacy of the PHI.

- Breach excludes:
  - Any unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use of disclosure in a manner not permitted under subpart E of [45 CFR §164].
  - Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of [45 CFR §164].
  - A disclosure of protected health information where a covered entity or business associate has a good faith belief that an authorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- Except as provided in the above paragraph of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    - The authorized person who used the protected health information or to whom the disclosure was made;
    - Whether the protected health information was actually acquired or viewed; and.
    - The extent to which the risk to the protected health information has been mitigated.

- There are state and federal laws we must follow for breach notification.

- Once you even suspect a breach of privacy, the law treats it as being “discovered.” Once discovered, time is limited by law to act upon a breach without penalty. This is why it is important that you immediately report any breach to Vidant Health Risk Management at 252-413-4473.
Policy/Process: Identity Theft Protection
Critical Elements:
- The Federal Trade Commission (FTC) has issued a set of regulations, known as the “Red Flags Rule,” requiring that hospitals, doctors’ offices and other entities develop and implement a written identity theft prevention program sufficient to detect, prevent, and minimize the damage that could result from patient identity theft.
- Vidant Health has established policies and procedures for staff members to follow to ensure Vidant Health protects patient’s medical and financial records in compliance with various federal and state identity theft laws, including the Red Flags Rule under the Fair and Accurate Credit Transactions Act.

Policy/Process: Release of Information
Critical Elements:
- There are no restrictions on Release of Information for treatment related purposes.
- The majority of releases of information should be referred to and managed by HIMS/Medical Records.

Policy/Process: Patient Right to Request an Amendment to the Designated Record Set
Critical Elements:
- Patients have a right to request an amendment to their Protected Health Information (PHI).
- Our organization has the right to deny their request.
- We must have documentation of the process used to make the request and take any action on it.
- Any requests for amendment should be referred to HIMS/Medical Records.

Policy/Process: Patient Right to Request Access to their Designated Record Set
Critical Elements:
- Patients have a right to request access to their Protected Health Information (PHI)
- Our organization must document the process used to make the request and take action on it.
- Any requests for access should be referred to HIMS/Medical Records.

Policy/Process: Clearance/Separation Process
Critical Elements:
- Managers must ensure that each employee completes the separation clearance checklist prior to their last day of employment.

Policy/Process: Confidentiality
Critical Elements:
- Patient information can be shared without restriction for treatment related purposes.
- Sharing of Protected Health Information must be limited to the minimum necessary data to perform the job expectation.
- There are significant consequences for inappropriate use or access of Protected Health Information up to and including dismissal, as well as severe civil and criminal penalties.

Policy/Process: Privacy Complaints
Critical Elements:
- Patients have a right to make a complaint to Vidant Health and to the federal government if they feel that their privacy has been breached.
• Vidant Health must inform patients in our Notice of Privacy Practices who they can make a complaint to in our organization and also of the right to make a complaint to the Secretary of Health and Human Services (DHHS).

• Privacy complaints need to be reported as soon as possible to the entity’s Privacy Officer. If after hours or on weekends, report should be made to Vidant Health Risk Management at 252-413-4473.

Policy/Process: Authorization form

Critical Elements:
• To be considered a valid authorization the form must contain the following elements:
  – Description of the information to be disclosed
  – Name of the person authorized to make the disclosure
  – Name of who the information can be released to
  – Purpose of the release
  – Expiration date
  – Signature of the individual
  – Date
• A separate authorization is available for research, psychotherapy notes and marketing

Policy/Process: Accounting of Disclosures

Critical Elements:
• We do not need to account for disclosures for treatment, payment and healthcare operations.
• We do not need to account for disclosures pursuant to an authorization.
• We must account to the patient for disclosures for a period of 6 years going forward from 4-14-03.
• We must account for disclosures such as public health, FDA, Health Oversight, law enforcement, state mandated registries and databases.

Policy/Process: Notice of Privacy Practices

Critical Elements:
• Must be given to each patient the first time they come to Vidant Health for service.
• Patients only need to receive it one time.
• This document outlines the patient’s rights and what we do with their Protected Healthcare Information.

Policy/Process: Privacy Policy

Critical Elements:
• Outlines the organizational philosophy of Vidant Health relating to patient privacy, confidentiality and use of Protected Healthcare Information.

Policy/Process: Overhead Paging

Critical Elements:
• It is a HIPAA violation to use a patient or family name when overhead paging unless it is an emergency situation.

Policy/Process: Document Destruction

Critical Elements:
• All PHI must be destroyed, shredded or de-indentified prior to leaving our facility.
• *Never* throw anything in the trash that identifies a patient; use the shred bins instead.

**Policy/Process: HIPAA Sanctions Policy**

**Critical Elements:**

- This policy will apply appropriate sanctions or disciplinary actions for employees who fail to comply with our HIPAA policies and procedures.
- The type of sanction will vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.
- The sanction applied shall be in accordance with our disciplinary action process outlined in the entity’s Employee Handbook, and range from counseling/re-education to immediate termination and reports to relevant licensing bodies.

**Policy/Process: Safeguarding Patient Information**

**Critical Elements:**

- All staff members are responsible for the protection of the medical record whether paper or electronic.
- Patient information should not be left displayed on computer screens, desks or workstations where unauthorized individuals can view.
- Nurse Managers and Department Managers will be ultimately responsible for safeguarding patient information on their units and for holding staff accountable for privacy breaches.

**Policy/Process: Printing Confidential Information**

**Critical Elements:**

- This policy outlines guidelines for printing confidential information when the user has a legitimate need to print information from a computerized Information System application.
- Printing of confidential information should be done for specific business purposes only and when viewing online will not suffice.
- Any failure to abide by this policy may result in loss of computer access, disciplinary action up to and including termination.

**Policy/Process: Privacy Complaint Process**

**Critical Elements:**

- A privacy complaint includes any complaint, whether presented in person, by telephone, in writing, or electronically, made by any individual regarding the HIPAA privacy policy and procedures or compliance with the HIPAA Privacy Rule in general.
- Privacy complaints may include a complaint about the way an individual’s patient information has been used or disclosed or a complaint regarding denial of access to patient information.
- All privacy complaints need to be called in to the Privacy Officer at each facility. If after hours or on weekends, contact Vidant Risk Management at (252) 413-4473.

**Policy/Process: Electronic Mail (E-mail) Use**

**Critical Elements:**

- Use of the Vidant Health e-mail system should be used for business purposes.
- Confidential information (including patient information) must be protected if sending via E-mail. This can be accomplished by entering the word “secure” in square brackets in the subject line.
  
  *Example:* [secure]
• The Vidant Health email systems and services are owned by Vidant Health, and are therefore its property. Vidant Health has the right to monitor any and all email traffic passing through its email system.

Policy/Process: Internet Use

Critical Elements:

• Internet use is intended for appropriate business and research purposes for acquiring, distributing, or exchanging information of administrative, medical, scientific, or technical nature only.

• Use of the Internet for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses) is prohibited.

• Use of the Internet in any way that violates Vidant Health’s Corporate Compliance policies, including but not limited to, viewing sexual content, sexual harassment articles or threats, etc., is prohibited.

• Internet access and use, from Vidant Health systems and services, are considered owned by Vidant Health, and are therefore its property. This gives Vidant Health the right to monitor any and all activity on the Internet.

Policy/Process: Workstation Use and Security

Critical Elements:

• Confidential and/or critical business information must be stored only on network attached storage devices. Confidential and/or critical business information must not be directly on the desktop device, unless required by the application, as information stored directly on workstations cannot be recovered if destroyed.

• Confidential information must not be stored on portable devices (flash drives, laptops, PDA’s, etc) unless the information is encrypted.

• Installation of unlicensed software is strictly prohibited and is subject to immediate removal by Information Systems (IS).

• Users are responsible for any and all access made under their user log-on. Users should not leave a workstation unattended when unauthorized persons can easily access confidential information. Temporarily logging off the application(s), or locking the active session is recommended.

Policy/Process: Device and Media Controls

Critical Elements:

• Storage media must be physically destroyed (drilling holes through storage media, cutting floppy disk and/or tapes, breaking or cutting CDs, etc.) or must have information irretrievably destroyed using IS approved sanitizing software, before being decommissioned or trashed.

Policy/Process: Security Incident Management

Critical Elements:

• Report suspected patient confidentiality security incidents to Risk Management.

• Report suspected computer virus infections, system or network intrusions, inappropriate use of your login identification to Information Systems (IS).

* * *
Shadowing Participants Name __________________________________________________________

Please Print

VIDANT HEALTH
HIPAA Training for the Observation Experience

By signing below I hereby certify that I have read, understand, and agree to abide by the attached HIPAA information relevant to my shadowing/observation experience.

_________________________________________  _______________________
Signature                                      Date

Revised 9/2013