VOLUNTEERS IN MEDICINE Hilton Head (VIM)

Annual Privacy and Security Training

VIM's PLEDGE

- We are proud of all our employees , volunteers, observers/students
- When you enter VIM, you are entering a world of patients and their very personal medical problems and identifying personal data
- We always need to be respectful of this responsibility. As we care for our patients, we need to follow all possible policies and rules that keep this information as safe as possible

WHAT GOVERNS THE PRIVACY AND SECURITY OF PROTECTED HEALTHCARE INFORMATION (PHI) IN THE U.S.?

1. **The Health Insurance Portability and Accountability Act (HIPAA) of 1996/2013**

2. **The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009**

3. **The 21st Century Cures Act of 2016**

These are the laws that your VIM Board, Director and Privacy and Security Officers follow to protect the healthcare data at VIM (The third Act mostly addresses research and adds very little to VIM issues)

WHY DO WE NEED RULES?

- These rules balance the flow of information required for excellence in healthcare while protecting the privacy and rights of our patients.

- Remember, it is more than just the law, it is about doing the right thing and preventing accidental and/or intentional misuse of our patients' private information.

What is Protected Health Information (PHI)?

PHI is generally any information in and from a health record, whether it is in paper/written, electronic or verbal form.

EXAMPLES OF PHI

1. Any encounter/visit documentation, note, etc. by any kind of staff - clinical or otherwise
2. Lab results, radiology films, any and all reports
3. Appointment data and times
4. Invoices and billing data
5. Any specific patient identifiers (see next slide)

EXAMPLES OF PHI (cont)

- Medical Record Numbers (MRNs)
- Social Security Numbers (SSNs)
- Account Numbers
- License/Certificate Numbers
- Vehicle/License Plate Numbers
- Personal IP and URL addresses
- Health Insurance Numbers
- Photographic images or voice files
- Birth dates or any dates specific to the individual
- Telephone and fax numbers
- Email addresses
- Biometric identifiers
- ANY OTHER UNIQUE CODE OR CHARACTERISTIC SPECIFIC TO THE PATIENT

WHAT ARE A PATIENT'S BASIC RIGHTS REGARDING THEIR PHI?

- Right to access their health care information (by in-person review or digital/paper copies)
- Right to request to amend their health information
- Right to request restrictions to sharing their information
- Right to request an accountability of any disclosures of their HPI
- Right to receive clinic or practice rules in a written, in plain language, in a Notice of Privacy Practices (NPP)
- Right to file a complaint with institution holding their PHI or with the Office of Civil Rights (OCR) in the Federal Justice Department

WHAT ARE VIM'S RESPONSIBILITIES?

- Not talking about patients outside of the office or even inside the office unless it is pertinent to their treatment and care. When one must talk about patients on the phone or in the office (and others are nearby) use as low or soft a voice as possible.
- Accessing patient information that is needed only for a particular activity related to clinic function and only when necessary.
- When releasing PHI under appropriate circumstances, releasing only the minimally necessary information required for the purpose.
- Keeping paper and electronic medical records as secure as reasonably possible during the work-day.
- Requiring specific, written permission to share any PHI outside of our operations unless it is for

  a. treatment, referral and continuity of their healthcare.

  b. billing/payment or research. (the latter under limited conditions)

  c. operation (for instance reporting, quality improvement, etc.)

  d. other specific instances such as child/elder abuse, public health disease reporting requirements, state vaccine and birth registers, court orders and subpoenas
- Informing patients of our intents to follow these practices by providing them with a Notice of Privacy Practices.

Some Specifics
FOR PAPER RECORDS

- Do not allow paper charts to be in places during work hours where they may be misused or viewed by inappropriate persons.
- Never take or allow paper charts to leave the VIM clinic complex.
- Never copy, mail, fax or email paper records without specific written permission, cover sheets and/or encryption. There are appropriate VIM staff trained to do this correctly, when indicated.
- Temporary or duplicate work notes or records that are not created to be part of the permanent chart AND contain any identifying data must be shredded or appropriately destroyed.
- When not in use, records must be in locked or in supervised areas.

Some Specifics
FOR ELECTRONIC RECORDS

- Each person at VIM must use a unique username and password (PW) to access any medical records required for patient care.
- VIM's current electronic medical record vendor requires this PW to be changed every three (3) months.
- Each record must be locked or logged out of if you leave an active workstation. Try to avoid letting non-VIM persons get a sustained view of your active work screen.
- You must NEVER share your unique password with others for any reason whatsoever. Seek help and advice from VIM staff if you have any difficulties.
- Never copy or export any electronic PHI unless it conforms with current privacy and security regulations. This should only be done by or under the supervision of trained VIM staff.
- Electronic health records are only to be destroyed under clinic policy by appropriate VIM staff or VIM contractors.
- VIM, as an organization, must assure that our "Business Associates" (partners who use or help us manage our PHI) also follow all appropriate rules and regulations.
- Access to VIM electronic PHI outside of the clinic complex and with equipment not owned by VIM is only allowed with special approval and access procedures.
- Users of VIM computers and hardware must never open any suspicious or unidentified email or email attachment. Always download any software or other material with extreme caution. Contact the security officer immediately if you suspect your computer has been compromised.

Some Specifics
FOR ALL CHARTS AND ANY PROTECTED HEALTH INFORMATION

- DO NOT access information on yourself, your family, your friends, your staff or ANY other person unless you are assisting in rendering healthcare through VIM.
- You have a legal duty to report any breach in security, privacy or confidentiality in any form to a supervisory VIM Staff member.
- Penalties for breaches are covered by VIM policy. Accidental and inadvertent breaches are usually remedied by reminders and re-education about policy and technique. Intentional or repeated breaches may result in counseling, reprimand or dismissal for the most egregious behavior.

SPECIAL CONSIDERATIONS

- In this new age of social media, everyone needs to be extremely cautious and follow these practices to remain compliant with privacy and security guidelines.
  a. **Never** take a picture with a personal phone or camera of anything pertaining to the patient's image or their medical record.
  b. **Never** put or post any such information anywhere – specifically no internet or social media site.
  c. Unless one is already a close friend or social media friend with a known patient, **never** try to access any of their online data,"befriend or ask to befriend" them or do anything else that would breach your knowledge of them as a client or patient at VIM. **Professional behavior** is the norm at all times.

Common Sense Can Also Prevail

HIPAA and other Federal and state privacy law never intended to entirely prohibit “inadvertent” disclosures of small pieces of patient information, if that is what is needed to operate a functional and safe medical practice. The following activities are NOT considered a violation of confidentiality rules.

1) **Calling patients by their name in a waiting room.**
2) **Patients signing in at a list or roster at the front desk**
3) **Patients and personnel passing by paperwork or computer screens as they go through normal office workflow (but allow no one to linger over the records with time and opportunity to read or copy)**
4) **Leaving non-specific messages on answering devices such as appointment reminders or requests for a return phone call.**

Always ask a supervisor if there is any question about what to do in new or uncertain circumstances.

CONTACTS FOR QUESTIONS, INFORMATION AND REPORTING AT VIM

Privacy Officer

Dottie Byers

Phone: 843-681-6612 Ext. 240

Email: dbyers@vimclinic.org

Security Officer

Demetra Ladson

Phone: 843-681-6612 Ext. 247

Email: dladson@vimclinic.org

WE HOPE YOU LEARNED A LOT

TAKE A LITTLE TEST FOR US

1. You should only access a patient's medical record if you need to do so for your duties at VIM.

A. TRUE

B. FALSE

TRUE - A health care worker or volunteer only has the right to see protected health information if it is needed to care for the patient.

2. It is OK to share information with family or friends even if you don't have the patient's permission.

a. TRUE

b. FALSE

FALSE – Patients have the right for their information to be limited only to their health care providers, their staff and others that the providers enlist in care, testing or billing, UNLESS a patient specifically indicates otherwise.

3. It is okay to share your password with a coworker who just needs to quickly “look something up.”

a. TRUE

b. FALSE

FALSE - There is NO situation when your own password should be shared with another.

4. All suspected privacy and information security incidents should be reported to the Privacy Officer, Security Officer or a supervisor.

a. TRUE

b. FALSE

TRUE - It is your legal responsibility to report any breach in your organization's operation that would endanger the privacy of protected health information.

5. At initial registration, patients are provided with VIM's Notice of Privacy Practices that explains, in plain language, how their health information may be used.

a. **TRUE**

b. **FALSE**

True - All health care entities are required to do this.

6. You may access any PHI you want if you are a health care employee or volunteer, even if the person is not your patient.

a. **TRUE**

b. **FALSE**

False – As an employee or volunteer of VIM, you must have a reason to be accessing a patient's protected information.

7. Which of the following are good practices to follow at your workstation?

a. **Logging off your system at the end of the day and whenever you leave your computer unattended**

b. **Writing down your password and pasting it on top of your screen**

c. **Facing monitors away from public view or using a privacy screen if they are near busy areas**

d. **a. and c. above**

e. **None of the above**

d. – NEVER write down your password in any obvious or unprotected place. Choices a. and c. are good work practices.

8. If a paper containing PHI is no longer needed, it should be placed in the regular trash container immediately.

a. **TRUE**

b. **FALSE**

False - Any paper containing PHI which is not part of the patient's clinical chart, needs to be disposed of by shredding, burning or other legal means established by the health care provider.

9. A patient has the right to request a copy of their health record.

a. **TRUE**

b. **FALSE**

True - A patient always has the right to request a part or all of their health record.

10. It would be permissible under current privacy regulations for you to look up a coworker's address in the electronic medical record so you can send the coworker a get-well card.

a. TRUE

b. FALSE

False - Information in a patient's health record is private and only accessible if you have a need to know in order to do your job. Look for that information elsewhere - by asking a mutual friend or colleague or looking it up in a public information base.