Privacy and You

Through compliance with federal laws and regulations as well as VA and VHA polices, you can be a part of the VA and VHA’s efforts to provide our Veteran’s the confidentiality they deserve.

INFORMATION PROTECTED UNDER PRIVACY ACT AND OTHER PATIENT PRIVACY STATUES

The Privacy Act as well as the five other statues govern the maintenance, collection and release of information seek to protect individually identifiable and health information.

Individually Identifiable Information

Includes: name, address, phone number, medical record number, social security number, photograph, billing and other account numbers, date of birth, date of visit, fingerprints.

Health Information

Includes: medical records/charts, billing information, lab tests results, x-ray and films, diagnosis and treatment, records, flow sheets.

Confidentiality of Certain Medical Records, 38 USC 7332

Includes records of the identity, diagnosis, prognosis, or treatment of any patient or subject which are maintained, relating to treatment of drug abuse, alcoholism alcohol abuse and sickle cell anemia and testing or treatment of HIV. PHI falling under these categories can only be disclosed with the patient’s written authorization or if permitted by the 38 USC 7332. Contact the Privacy Office to ensure appropriate authority when disclosing without the patient’s written authorization.

GENERAL KNOWLEDGE

• Be able to identify the Privacy Officer and Information Security Officer.
• Comply with Health Care System Memorandum and VHA/ VA Policies, Handbooks and Directives relating to privacy and information security.
• Access information only as necessary for your official job responsibilities.
• Report suspected privacy/info security violations promptly.
• Do not be afraid to ask questions about practices.
• Do not use patient information for personal gain.
• Log off computer and remove PIV card when leaving your work station and out of eyesight from your computer.
• Cooperate fully during fact findings.

When Providing Treatment

• Close doors when discussing or providing treatment.
• Close curtains and speak softly in semi-private rooms when providing treatment.
• Remove patient information from treatment room after visit has ended.
• Using cell phones to take photographs of patient wounds or other treatment areas is not allowed. Authorized cameras are available and instructions for uploading into the medical record is provided through proper channels.

Public Areas & Auditory Privacy
• Avoid discussion about patients in public areas (elevators, canteen, waiting areas, corridors, stairwells, etc.)
• Don’t leave PHI on desk, counters or workstations where others can easily view.
• Use an appropriate tone of voice when you’re speaking with a veteran in a public area, such as during the check-in process, to ensure protection of patient privacy.

Phone Messages
• To reasonably safeguard the individual’s privacy, limit the amount of information disclosed.
• Only leave your facility name and number and other information necessary to confirm an appointment or ask the individual to call back. Do not disclose the clinic name or protected health information.

Faxes
Fax sensitive information only when mail delivery is not fast enough to meet patient needs, and double check that information was sent to correct fax number.

Email
• Email message can only include PHI if the message is full encrypted (ex: PKI or RMS). Be sure to check that PHI is not included in the subject line.
• Provider to patient emailing is prohibited. Use the secure messaging application in MyHealtheVet for all communications to patients that involve PHI.

Photo ID - PIV Card Usage
Wearing your VA photo identification badge, PIV card, is critical to effective hospital privacy and security programs. HCSM 07B-5 mandates all employees, contractors, volunteers, medical residents, students and trainees wear the badge issued by our facilities. Badges are to be worn above the waist with front (photo side) visible.

HIPAA – Minimum Necessary
The HIPAA Privacy Rule protects Protected Health Information (PHI) in all forms, and sets standards all Covered Entities and their employees, contractors and students must meet to protect patients’ confidential medical records. The HIPAA Security Rule deals exclusively with PHI in electronic form that is used, stored, and transmitted by electronic devices and networks. The Minimum Necessary Standard states that when using or disclosing PHI, or when requesting PHI from another covered entity, the provider must make reasonable efforts to limit PHI to minimum necessary to accomplish intended purpose for use, disclosure or request.
Official Requests for Information
All official requests for information (excluding those for medical records) from such entities as Inspector General, local/state/federal law enforcement agencies, attorneys, general public, etc., should be referred to the Privacy/FOIA Officer for processing.

Electronic Medical Records
HIPAA protections extend to any identifiable information related to the “past, present or future physical or mental health condition.” You should NEVER access or disclose any of the below without proper justification or authorization from the patient! Only staff who are directly involved in providing treatment, payment or other healthcare operations (TPO) are authorized to access patient information.

Information that is protected:
- Patient names, Social Security numbers, names of relatives, health plan numbers
- Dates of service, patient history, discharge summary, progress notes, allergies
- Pictures, phone numbers (telephone, fax), email addresses, zip codes
- No snooping allowed! Having access to CPRS is not a blanket authority to enter a record without a “need to know!” When in doubt, ask yourself:
  - Am I providing treatment?
  - Am I answering a question or providing results?
  - Is this part of my official job duties?
  - Am I coding or billing?
  - Am I providing program oversight?
  - Or, am I just being nosy?

Do not access another employee’s medical record without proper authority, even if that employee requests it. If you do not have a justifiable reason, one that can be tracked during a fact-finding, you should not enter the record! Not only is it unethical, it’s a punishable violation. Refer your coworker to Release of Information department (ROI).

IMPAIRED DRIVERS
When a patient is an impaired driver, any intervention undertaken should be in accordance with what is in the best interest of the patient and should honor the physician patient relationship. Staff should disclose to patients their responsibility to take steps to intervene and perhaps to discuss with family members involved in the patients care their impairment to drive. Staff are not allowed to report impaired drivers to the DMV without the patients written and signed authorization.

TO REPORT A PRIVACY CONCERN/VIOLATION
Immediately take steps to secure information at risk. Report the observation to the Privacy or Information Security Officer as soon as possible, notating specifics; after normal business hours of 8:00 a.m.-4:30 p.m., Mon- Fri, contact the Administrative Officer of the Day (AOD) at 402-995-5937, with details. For non-emergencies, you may leave a voicemail, email us or contact the AOD. You may anonymously make a report.
REMOVING OR TRANSPORTING PROTECTED INFORMATION OUTSIDE OF VA PROTECTED ENVIRONMENT
Employee’s requesting to remove protected information outside of VA protected environments MUST have VA “Authorization to Transport” form completed, and signed by all individuals before removal of any information or equipment from VA protected environments, per VA Directive 6500. Failure to complete this form may result in a privacy and information security violation. Protected information includes: Individually identifiable medical; Benefits or personal information; Information that can be withheld under the Freedom of Information Act; Financial Information; VPN/Laptop Access; Mobile Media (all removable, Mobile/Portable/Wireless and Storage Devices); Research Information; Investigatory Information; Commercial Information; Quality assurance information; Law enforcement information; Information that is confidential or privileged in litigation; Information that could adversely affect the national interest or conduct of federal programs. To obtain the form, contact the Privacy or Information Security Office.

VETERANS MAKING SERIOUS THREAT TO HEALTH OR SAFETY OF OTHERS
Scenarios where a patient has made a credible threat to the health or safety of an individual, such as a spouse or a public figure. Disclosure of protected health information (excluding 38 U.S.C. 7332 information) in such situations is allowed, if the requirements of the privacy laws are followed. Contact the Privacy Officer to ensure compliance with federal laws.
• Serious or imminent threat to self: Disclosure should be made to the nearest local police department immediately to prevent or lessen the threat to the individual. (e.g., suicidal Ideation or cannot get in contact with Veteran) Contact the Privacy Officer AFTER you call the welfare check to police.
• Threat to family member: Disclosures may be made to a family member of a patient when it is necessary to prevent or lessen a serious or imminent threat to the health or safety of the family member. Disclosure may also be made to local authorities who may be able to prevent or lessen the threat. Contact the Privacy Officer prior to disclosing information outside of the VA.
• Threat to public at large: Disclosures may be made to a person or persons reasonably able to prevent or lessen a threat made to the health or safety of the public (e.g., Police Department regarding bomb threat) Contact the VA police and Privacy Office.
• Threat to national security: Disclosure may be made to law enforcement authorities to identify or apprehend an individual making serious threat against the nation (e.g., FBI regarding terrorist activity) Contact the VA police and Privacy Office.

FREEDOM OF INFORMATION ACT (FOIA)
What is Freedom of Information Act (FOIA)?
• The basic purpose of the FOIA is “to ensure an informed citizen, vital to the functioning of a democratic society, needed to check against corruption and to hold governors accountable to the governed.”
• The FOIA establishes a presumption that records in the possession of agencies and departments of the executive branch of the U.S. Government are accessible to the people.

What are Employee Responsibilities under FOIA?
• All employees, contractors and students are required to fully cooperate in the handling of FOIA requests as directed by the local FOIA Officer. Specific employee responsibilities include:
  • Searching for agency records at the direction of the local FOIA Officer.
  • Fully documenting the FOIA search efforts to include time spent searching, search terms utilized, and identification of systems or files searched.
  • Providing responsive records to the FOIA Officer in a timely manner, this includes providing records in the format requested by the requestor, if available.
  • Being accessible to the FOIA Officer for questions/clarifications.
  • Fee estimates at the direction of the FOIA Officer.
  • Employees, contractors and students should not contact a FOIA requestor.
  • All communications with a FOIA requestor must be made by the FOIA Officer.