Volunteer Privacy and information security Training

VA San Diego Healthcare System

January 2017

Information security Training

- - Don’t send personal health information (PHI) through email unless the information has been de-identified or encrypted.

- -De-identification involves removing all patient identification information including name, SSN, address, date of birth, medical information, etc.

- When sending a FAX, make sure phone number is correct, include cover page, give faxes to your supervisor in a timely manner.

Information security Training continues

- - When leaving a message, give office and phone number for patient to call back, do not talk about any personal health information pertaining to Veteran.

- - When disposing of documents or items make sure the patient's name and other information is not able to be read.

- - Place all documents with identifiable information in shredder or locked box designated for shredding.

Privacy Training

- - Always relay the minimum amount of patient information necessary to take care of the emergent situation at hand to the supervisor in the area.

- - Emergent situations include:
  - Bleeding
  - Shortness of Breath
  - Assault
  - Suicide threats
  - Chest pain
  - Missing patient

Privacy Training part 1

- Opt Out Information

- - Opt Out information applies to information that the patient does not want released during his/her hospital stay.

- - Do not release information to anyone such as visitors, phone callers, mail delivery, etc. Check with your supervisor before giving out information.

Privacy Training Part 2

- - Speak in a low voice in public areas.
- - Use private areas whenever possible when speaking about patient information.
- - Under no circumstances discuss patient information with anyone that does not need to know.
- - Do not discuss patient health information in elevators, cafeterias, or other public places.

More Information Security Training

- - If you are authorized to use the VA computer during your volunteer assignment:
  - Only look at information that is necessary to do your job.
  - Do not place computer codes or volunteer sign in codes on back of badge, in plain view, or under keyboard.
  - Do not share codes with others; each volunteer must log in under their own code.

Health Insurance Portability and Accountability Act (HIPAA)

- The HIPAA Privacy Rule provides confidentiality for VA patients' protected health information (PHI). The Privacy Rule:
- Authorizes VA to use or disclose information without a patient's prior written authorization for VHA treatment, payment or health care operations.
- Prohibits other uses and disclosures of PHI except as authorized by the regulation or with a prior written authorization.
- Provides rights to the individuals to whom the PHI pertain.

Incidental Disclosures

- Privacy policy allows for the following incidental uses and disclosures of individually identifiable health information in certain circumstances:
  - Posting patient names outside rooms.
  - Bingo Boards (with limited information).
  - Patient sign-in sheets (no SSN or diagnoses).
  - Calling only the patient's name in a waiting area.
  - Ward "white boards" (with limited information).
  - Curtains dividing treatment areas in emergency areas instead of separate rooms.

Minimum Necessary Standard

- Requests for, and disclosures of, health information must be limited to only the minimum amount necessary to accomplish the needed purpose.
- Healthcare providers must be given what is needed for treatment including continuity of care of the individual.
- For other than treatment purposes, where VHA employees are authorized access to protected health information (PHI) to perform their VHA duties, they may have access to only the minimum necessary PHI to perform their VHA duties

Veterans' Privacy Rights

- VA patients have several Privacy Rights in their VHA patient records, including the right to:
  - Receive a notice of VHA's privacy practices,
  - Request access to his/her VHA medical records,
  - Request restrictions on VHA's use and disclosure of the records,
  - Request that VHA amend the medical records,
  - Request an accounting of VHA's disclosures of the records,
  - Ask VHA to communicate with the patient about his medical care in certain agreed methods, and
  - File a complaint about any VHA conduct with the patient's PHI that the patient believes violates the HIPAA Privacy and Security Rules.

Veterans' Notice and Access Rights

- **Notice of Privacy Practices:** VA must periodically notify Veterans in writing how VA may use or disclose their protected health information, how they may exercise their privacy rights and how they may submit privacy complaints.
- **Access:** Veterans have the RIGHT to request and receive copies of their records. Facilities should infrequently deny access requests. Access requests must be processed as stated in VHA Handbook 1605.1, paragraph 7. The Veteran must be notified of any denial of access in writing and provided appeal rights.

Penalties for unauthorized disclosure of patient information:

- Civil penalties: $100 per violation, up to $25,000 per person, per year for all violations of a requirement.
- Criminal penalties for **knowing violations** include:
  - Up to $50,000 and one year in federal prison.
  - Under "false pretenses" – up to $100,000 and up to five years in federal prison.
  - "Intent to sell, transfer or use" – up to $250,000 and up to 10 years in federal prison.
- In addition to the penalties listed above, administrative, disciplinary or other adverse actions (e.g., admonishment, reprimand or termination) may be taken against volunteers who violate any of the applicable legal provisions.

Examples of Privacy Breaches

Accessing confidential information that is not within the scope of your duties:

- Unauthorized reading of patient account information;
- Unauthorized reading of a patient's chart;
- Unauthorized access of personal file information;
- Accessing information that you do not have **"need-to-know"** for the proper execution of your duties.

Privacy Breach Examples

Intentional or negligent mishandling or destruction of confidential information:

- Leaving confidential information unprotected and unattended at your work area;
- Leaving confidential information in areas outside of your work area, such as the cafeteria, other public places within the Clinics or your home;
- Disposing of confidential information in a non-approved container, such as a trash can, recycle bins, etc.