



# VHA Privacy Policy Training FY 2011





# Applicable Confidentiality Statutes and Regulations

- The following legal provisions govern the collection, use, maintenance, and disclosure of information from VHA records.
  - The Freedom of Information Act (FOIA) (5 U.S.C. 552)
  - The Privacy Act (5 U.S.C. 552a)
  - 38 U.S.C 5701 - The VA Claims Confidentiality Statute
  - 38 U.S.C 7332 - Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records
  - 38 U.S.C. 5705 - Confidentiality of Healthcare Quality Assurance Review Records
  - The HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164



# Freedom of Information Act (FOIA)

- FOIA compels disclosure of reasonably described VHA records or a reasonably segregated portion of the records to any person upon written request, unless one or more of the nine exemptions from the general disclosure requirement apply. Generally, VHA is not required to release individually-identifiable veteran information under FOIA.
- Contact your facility FOIA Officer if you receive, or have questions regarding, a FOIA request.



# Privacy Act of 1974

- Provides for the confidentiality of information about an individual that is retrieved by the individual's name or other unique identifier, such as the SSN.
- Such information is contained in a system of records and must be protected.
- Prohibits disclosure of any record contained in a system of records unless specifically authorized by the Act.
- Provides rights to the individual by whose name VHA retrieves the information.
- Contact your facility Privacy Officer with questions regarding the Privacy Act and systems of records.



## 38 U.S.C 5701 (VA Claims Confidentiality Statute)

- Provides for the confidentiality of all VHA patient claimant information, with special protection for their names and home addresses.
- Provides for the same for information about their dependents.
- Prohibits disclosure of these names and addresses except as authorized by the statute.
- Does not apply to employee information.



## 38 U.S.C 7332

- Provides for the confidentiality of VHA-created, individually-identifiable Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records and Health Information.
- Prohibits use or disclosure with a few exceptions. VHA may use the information to treat the VHA patient who is the record subject.
- Must have specific written authorization in order to disclose in most cases, including for treatment by non-VA provider.



## 38 U.S.C 5705

- Provides for the confidentiality of Healthcare Quality Assurance (QA) Review Records.
- Records created by VHA as part of a designated medical quality-assurance program are confidential and privileged.
- VHA may disclose this data in only a few, limited situations.
- Contact your facility Privacy Officer if you collect QA data, or have questions concerning the use or disclosure of section 5705-protected information.



# Health Insurance Portability and Accountability Act (HIPAA)

- The HIPAA Privacy Rule provides confidentiality for VHA patients' protected health information (PHI). The Privacy Rule:
- Authorizes VHA 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.



# Payment

- A payment is an activity undertaken by VHA to determine its responsibility for coverage or to provide reimbursement for health care.
- This could include pre-certification, utilization review or release of protected health information (PHI) to a third party insurance carrier for VHA reimbursement for care provided.



# Treatment

- Treatment is defined as the coordination or management of health care or related services by one or more health care providers. VHA is a health care provider.
- This includes the coordination of health care by a health care provider with a third party, consultation between providers relating to a patient and the referral of a patient for health care from one health care provider to another.



# Health Care Operations

- Health care operations are those activities which are deemed essential to the effective operation of a VHA medical facility.
- These include conducting quality assessment and improvement activities, case management, reviewing competence or qualification of health care professionals, evaluating practitioner performance, legal services, business management, auditing and customer service evaluations.



# Relationship between Laws

- VHA employees must comply with all applicable privacy laws and regulations when:
  - Accessing, using or disclosing information, and
  - Processing requests from individuals exercising their privacy rights.
- When conflicts arise:
  - The more stringent law or regulation applies for uses and disclosures,
  - The one that affords the greatest rights to the individual applies for privacy rights.
- Reference VHA Handbook 1605.1, Privacy and Release of Information, and/or contact your facility Privacy Office if you have questions.



# Compliance with Privacy Policies

- All employees must conduct themselves in accordance with the rules of conduct concerning the disclosure or use of information.
- All employees and some contractors must sign the Statement of Commitment and Understanding.
- VHA privacy policy is contained in VHA Directive 1600 and VHA Handbook 1605.1, Privacy and Release of Information.
- Failure to comply with privacy policies could lead to significant civil penalties for the agency and disciplinary or other adverse action or criminal penalties for the employee.



# Use of Information

- Remember, VHA employees must comply with all six statutes and regulations, where applicable, when using, accessing or disclosing information.
- VHA employees may access information in order to perform their official duties related to the treatment of veterans, the payment for care provided by VHA and/or the health care operations of VHA.



# Incidental Disclosures

- Privacy policy allows for the following incidental uses and disclosures of individually identifiable health information:
  - Posting patient names outside rooms
  - Pharmacy 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
- Contact the facility Privacy Officer with questions whether other conduct may be an incidental disclosure.



# Disclosure of Information

- VHA generally is not obligated to release information
- The general rule is that the use or disclosure of protected health information is prohibited unless authorized by all applicable confidentiality statutes and rules. Commonly permitted disclosures include:
  - For treatment, payment or health care operations
  - Authorized by the patient, or
  - Required for public health and/or certain law enforcement purposes, or
  - Where required by law, including pursuant to a qualifying court order.



# What can be Disclosed?

- Under some circumstances, it is necessary for non-ROI staff to release information. Written requests must be obtained from the requestor so that these can be accounted for in the ROI software.
- Clinicians may provide information directly to a patient for purposes of patient education without obtaining a written request.



# Authorization Requirement

- Any authorization for release of medical information must be in writing and contain all required elements. Verbal authorizations are unacceptable under applicable Federal law.
- Most requests for records should be processed by the Release of Information (ROI) Unit.
- VA Form 10-5345 Request for and Authorization to Release Medical Records or Health Information meets the authorization requirements.
- VA Form 10-5345a Individuals Request for a Copy of their Health Information meets the written request requirement when veterans request copies of their own health information.



# Exception to Need for Authorizations

- There are situations where a disclosure may be made without an authorization. For example, Public Health Reporting.
  - Disclosure to Public Health Authorities charged with protection of the public may be done only with a standing written request or other applicable legal authority.
- Contact your facility Privacy Officer for additional information on situations where an authorization is not required.



# Research

- VA Research requests must have approval from the Research & Development Committee and an Institutional Review Board (IRB).
- Because the privacy requirements to use health information for research are complex, the facility Privacy Officer or Research Compliance Officer should be contacted for assistance.
- For further information review VHA Handbook 1605.1 Privacy and Release of Information, paragraph 13.



# 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
- Contact your facility Privacy Office for more information.



# Functional Category

- Each employee must have a functional category assigned to them:
  - Functional Categories identify the appropriate level of access to protected health information
  - See VHA Handbook 1605.2 Minimum Necessary Standard for Protecting Health Information



# Facility Directory Opt-Out

- Except in limited circumstances, a VHA facility will ask a patient upon admission whether s/he wishes to be in the Patient Facility Directory.
- If the patient does not object, the facility may tell anyone who asks for the patient by name the patient's name, location and general medical condition.
- If the patient objects to inclusion in the Directory, the facility identifies the patient by "!" on Gains and Losses report and in VistA Patient Inquiry, and Cannot release any information whatsoever to anyone who asks for the patient- say, "I am sorry but I have no information that I can give you whether Mr. X is a patient."
- Patients may change their mind about being in the Directory at any time during their admission.



# 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.



# Veterans' Right to Request Restrictions

- **Restrictions**: Veterans have the right to request restrictions on the use and disclosure of their information.
- The request must be in writing and signed by the veteran; however, VHA is not required to grant restriction requests. You are to follow the procedure in VHA Handbook 1605.1, paragraph 11 in processing requests for restrictions. In most cases, such requests will be denied.



# Veterans' Amendment Right

- **Amendments**: The veteran has the right to request an amendment to any information in his/her record.
- The request must be in writing and adequately describe the specific information the veteran believes to be inaccurate, incomplete, irrelevant or untimely, as well as the reason for this belief.
- All requests for amendment will be reviewed by the facility Privacy Officer and the author of the information being disputed by the veteran.



# Amendment Continued

- The veteran must be notified of any denial of amendment in writing and provided appeal rights, the opportunity to file a statement of disagreement, and the opportunity to have his original request letter and the facility denial letter attached to the disputed information if a statement of disagreement is not filed.



# Veterans' Accounting Right

- **Accounting of Disclosures**: VHA medical facilities are required to keep, and a veteran may request, a list of all disclosures of information, both written and oral, from records pertaining to the individual, subject to certain legal exceptions.
- Accountings are not required when the information is requested for performance of official VHA employee duties.
- VHA Handbook 1605.1, paragraph 9 has more information on Accounting.



# Veterans' Request for Confidential Communications

- **Confidential Communications**: An individual has the right to request and receive communications confidentially by an alternative means (for example, in person) or at an alternative location (address other than the individual's permanent address)
- Current VHA policy is not to honor a request to receive communications via e-mail because currently e-mail exchanges with patients are not sufficiently secure to protect the information.



# Veterans' Right to File a Complaint

- **Right to File a Complaint**: Patients may file a written complaint about VHA's handling of the patients' information with the facility Privacy Officer, the Office of Inspector General, the VHA Privacy Office or with the Department of Health and Human Services, Office for Civil Rights.
- The facility must respond in writing to the complainant and put the information into the Privacy Violation Tracking System (PVTs).



# HHS Privacy Complaints

- If a VHA facility receives a complaint directly from the Department of Health and Human Services (HHS) Office for Civil Rights, contact the facility Privacy Officer immediately.
- The facility Privacy Officer will contact the VHA Privacy Office and VHACO.
- Contact the VHA Privacy Office to coordinate all responses to a complaint.



# Training

- A new VHA employee must receive VHA privacy training within 30 days of entrance on duty.
- All VA employees must complete privacy training annually.
- “Employees” include FTEE, consultants and attendings, without compensation, fee basis, contractors, students and volunteers.
  - CWT workers are not considered employees and cannot access individually-identifiable patient information without the facility first obtaining proper written authorization from the patient.



# Penalties

- 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 employees who violate any of the applicable legal provisions.



# Operational Privacy Issues

- **Faxes**: Information may only be faxed when:
  - No other means exists to provide the requested information in a reasonable manner or time frame;
  - The fax machine is in a secure location; and
  - Reasonable steps have been taken to ensure the fax transmission is sent to the appropriate destination.
- **Email**: No protected health information (PHI) should be sent unencrypted via Outlook. PHI should be encrypted prior to transmission by using VHA-approved means.



# Reasonable Safeguards

- **Computer security:**

- Log off or lock work station
- Turn computer screen/monitor so it is not visible by people passing by
- Secure passwords

- **Office Security:**

- Protect information that is on your desk
- Lock doors to rooms containing medical records
- Lock file cabinets containing health information or other individually identifiable information (employee or veteran)



# Reasonable Safeguards

- **Document Shredding**: **NO** protected health information should be discarded in regular wastebaskets. All confidential information should be shredded to ensure patient privacy.
- **Open Discussions**: Absolutely **NO** health information should be the topic of discussion outside the clinical setting. This includes in places such as the hallway, the canteen, elevators or the parking lot.



Protecting the privacy of veterans' information is an important part of providing quality health care AND is everyone's responsibility.



# 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.



# Examples of Privacy Breaches

**Disclosing to another person your sign-in code and / or password for accessing electronic confidential information or for physical access to restricted areas:**

- Telling a co-worker your password so that he or she can log in to your workstation for any purpose;
- Telling an unauthorized person the access codes for personnel files, patient accounts or restricted areas;



# Examples of Privacy Breaches

**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 Medical Center or your home;
- Disposing of confidential information in a non-approved container, such as a trash can, recycle bins, etc.



# Examples of Privacy Breaches

**Attempting to access a secured application or restricted area without proper authorization or for purposes other than official VA / VHA business:**

- Trying passwords and login codes to gain access to an unauthorized area of the computer system or restricted area;
- Using a co-worker's application for which you do not have access after he or she is logged in.



# Examples of Privacy Breaches

**Misusing, disclosing without proper authorization, or altering confidential information:**

- Making unauthorized changes in patient paper charts;
- Making unauthorized changes to a personnel file;
- Unauthorized reproduction of information in patient chart;
- Sharing information in a patient chart with unauthorized personnel/staff;
- Discussing confidential information in public areas such as waiting room, elevator, break room, etc



# Examples of Privacy Breaches

**Using another person's sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas:**

- Using a co-worker's password to log in to the Medical Center's Health Care Information Systems;
- Unauthorized use of a login code for access to personnel files, patient accounts, or restricted folders with sensitive information.



# Examples of Privacy Breaches

**Leaving a secured application unattended while signed on:**

- Being away from your desk while you are logged into an application;
- Allowing a co-worker to use secured application assigned to you after you have logged in - especially if he or she does not have access to it



# Examples of Privacy Breaches

**The examples shown above are only a few types of mishandling confidential information.**

**If you have any questions about handling , or disclosure of confidential information or general privacy issues, please contact Medical Center Privacy Officer.**



## **Privacy Officer**

Joseph Boateng, MHIM, RHIA  
Business Office, RM 6018 - 136F  
(901) 523-8990, ext. 7087  
pager: 717

## **Alternate Privacy Officer**

Maureen Wheeler, MPA, RHIA  
Business Office, RM 6018 - 136F  
(901) 523-8990, ext. 7859