Veteran Information Privacy Compliance 101:
For Iowa County Commissioners on Veteran Affairs Regarding Veteran Service Work

Presented by, Russell E. Saffell, Ph.D.(c), M.P.S.

September 2024

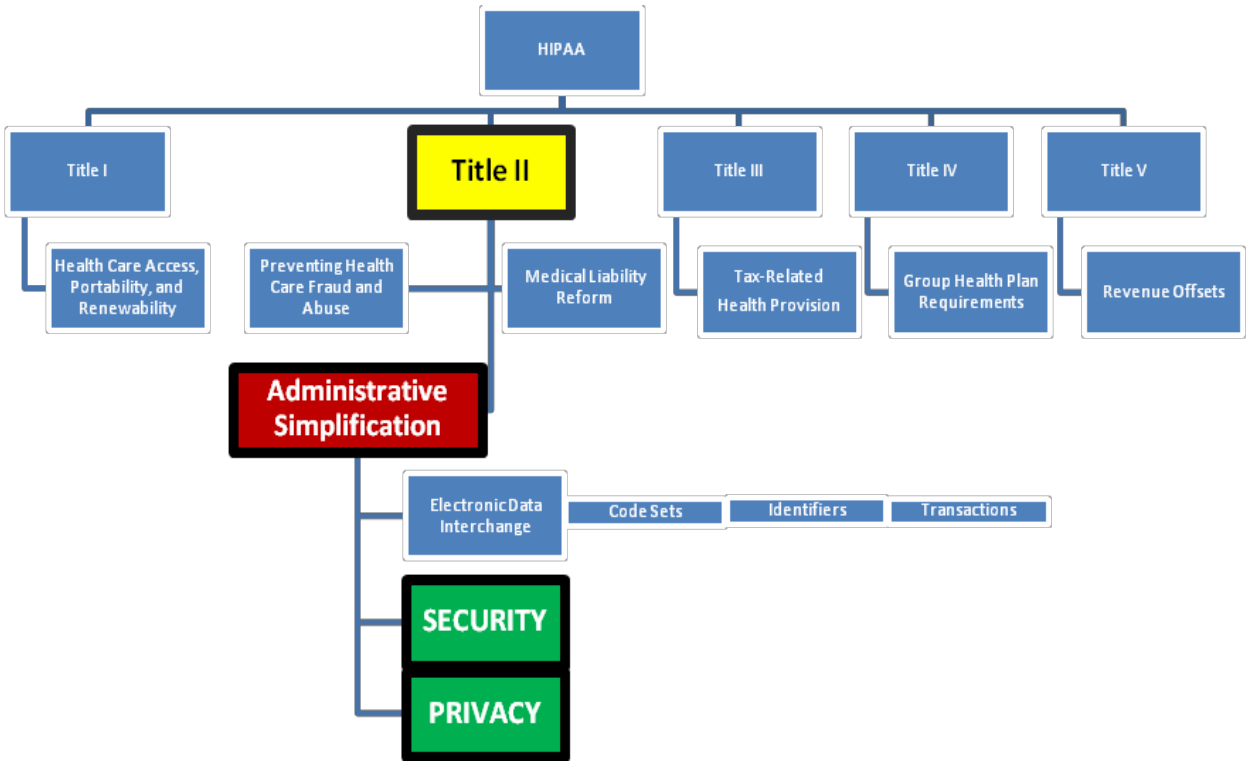
Overview

1. Discuss how HIPAA applies and does not apply to Veteran service work.
2. Discuss what other laws, rules, policies, etc. related to information privacy and security apply to CVACs & CVSOs.
    a. Detail compliance requirements.

What is HIPAA?

Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA)

- Passed by the 104th Congress in 1996
- Implemented in the Code of Federal Regulations (CFR)
- Privacy and Security, which align under Administrative Simplification, represent only two components of HIPAA.



What HIPAA Does:

The lay public usually thinks of "privacy" when they hear the word HIPAA, but in fact the purpose of HIPAA reaches much further, to include efforts to:

- Improve the portability and continuity of health insurance coverage
- Combat waste, fraud, and abuse in health insurance and health care delivery
- Promote the use of medical savings accounts
- Simplify the administration of health insurance

Who Must Comply with HIPAA:

Any individual or organization that meets the definition of a covered entity

- A simplified definition of a covered entity is: A health plan (e.g., TRICARE), a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction.

Business Associates must also comply with certain aspects of the HIPAA Rules

- A simplified definition of a business associate is someone who is not a member of the covered entity workforce but performs activities on behalf of the covered entity that involves the use or disclosure of protected health information.

The Requirements for Those Who Must Comply:

- Develop policies & procedures to ensure compliance with the HIPAA Privacy and Security Rules
- Enforce employee compliance with policies and procedures, to include sanctions (discipline) when required
- Develop and publish a Notice of Privacy Practices that explains patient's rights and how their health information will be used
- Ensure employees are trained on HIPAA requirements and understand how HIPAA is applicable to their work environment

So… HIPAA???

HIPAA and PHI are terms that get thrown around a lot whenever discussing health related information, but it is often misused.

- Do CVACs or CVSOs need to worry about HIPAA?

  - County Commissions of Veteran Affairs and CVSOs are not considered as HIPAA "Covered Entities" or "Business Associates"
  - County Commissions of Veteran Affairs and CVSOs are not bound by HIPAA, but have similar compliance requirements
- What about Protected Health Information (PHI)?
  - PHI only refers to information created, used, or disclosed by a healthcare provider that is a HIPAA covered entity
  - PHI ceases to be considered PHI when it is not being maintained by a HIPAA "Covered Entity" or "Business Associate", but that does not mean information with the same or similar markers are not required to be protected by CVSOs, just under entirely separate rules
- ***ARE YOU CONFUSED YET?***

Actual Compliance

What do CVSOs have to maintain compliance with?

- Privacy Act of 1974
- VA Policies and Guidance
- Policies of VA recognized service organizations (VFW, American Legion, DAV, etc.)

Privacy Act of 1974

The Privacy Act of 1974 (5 U.S.C. Sec. 552a) regulates the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy.

The Act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies
2. To grant individuals increased rights of access to agency records maintained on themselves
3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete; and

4. To establish a code of **"*Fair Information Practices*"** which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records

Fair Information Practice Principles (FIPPs)

FIPPS are a set of principles that guide how organizations handle personal information:

- **Collection:** Limit the collection of personal information
- **Data quality:** Ensure data is accurate and reliable
- **Purpose:** Specify the purpose for collecting and using personal information
- **Use:** Limit how personal information can be used
- **Security:** Use safeguards to protect personal information
- **Openness:** Be open about how personal information is handled
- **Individual participation:** Give individuals control over their personal information
- **Accountability:** Hold organizations accountable for complying with these principles

VA Privacy & Information Security Awareness and Rules of Behavior (RoB)

The VA has very robust FIP policies and procedures that CVSOs are also bound to comply with:

These are general ROBs that pertain to everyday behavior expected of Non-Organizational Users:

- I WILL comply with all Federal statutes, regulations, and policies applicable to VA information security, information privacy/disclosure, and records management policies. (SOURCE: PM-10)
- I WILL NOT have any expectation of privacy in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. (SOURCE: AC-10)
- I WILL complete mandatory security and privacy awareness training within designated time frames. (SOURCE: AT-2)
- I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)
- I WILL sign specific VA Information Security ROBs required for access or use of specific VA or non-VA systems. (SOURCE: AC-8)
- I WILL obtain approval from the Office of Public and Intergovernmental Affairs (OPIA) before establishing a VA social media account.

Ethics?

CVSOs are bound by the same ethical standards as attorneys!

The Standards of Conduct in 38 C.F.R. § 14.632

VA-accredited individuals providing VA claims assistance ***SHALL***:

1. Faithfully execute their duties on behalf of a VA claimant
2. Be truthful in their dealings with claimants and VA
3. Provide claimants with competent representation before VA; and
4. Act with reasonable diligence and promptness in representing claimants

VA-accredited individuals ***SHALL NOT***:

1. Violate the standards of conduct as described in 38 C.F.R. § 14.632.
2. Circumvent the rules of conduct through the actions of another.
3. Engage in conduct involving fraud, deceit, misrepresentation, or dishonesty.
4. Violate one or more of the provisions of title 38, United States Code, or title 38, Code of Federal Regulations.
5. Enter into an agreement for, charge, solicit, or receive a fee that is clearly unreasonable or otherwise prohibited by law or regulation.
6. Solicit, receive, or enter into agreements for gifts related to representation provided before an agency of original jurisdiction has issued a decision on a claim or claims and a Notice of Disagreement has been filed with respect to that decision.
7. Delay, without good cause, the processing of a claim at any stage of the administrative process.
8. Mislead, threaten, coerce, or deceive a claimant regarding benefits or other rights under programs administered by VA.
9. Engage in, or counsel or advise a claimant to engage in, acts or behavior prejudicial to the fair and orderly conduct of administrative proceedings before VA.
10. Disclose, without the claimant's authorization, any information provided by VA for purposes of representation.
11. Engage in any other unlawful or unethical conduct.