

Attachment C: Information Security Questions for Veterans Affairs (VA)

Date: Monday, October 28, 2013

Source: House Veterans Affairs Subcommittee on Oversight and Investigations

Scope: The Health Information Technology for Economic and Clinical Health Act (HITECH Act), issued in 2009

The House Veterans Affairs Subcommittee on Oversight and Investigations is currently examining the roles and responsibilities of VA's Office of Information & Technology (OI&T) in managing its information security initiatives. The Subcommittee is asking that VA answer the questions below designed to gather information regarding their efforts to address applicable federal legislation, standards, and guidance. This work reflects the continuing interest of the Subcommittee in preventing exploitation of Veterans' personally identifiable information (PII) and to improve VA's internal and external cyber security of Veterans' records.

We identified the following as either statutory requirements or as critical to effective information security management of PII and data breaches:

Legislation

Attachment A:	Date Sent: Wednesday, October 23, 2013	Date Due: Wednesday, November 6, 2013
----------------------	---	--

The Veterans Benefits, Health Care, and Information Technology Act of 2006

Attachment B:	Date Sent: Friday, October 25, 2013	Date Due: Friday, November 8, 2013
----------------------	--	---

Privacy Act of 1974

Attachment C:	Date Sent: Monday, October 28, 2013	Date Due: Monday, November 11, 2013
----------------------	--	--

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), issued in 2009

OMB Guidance (includes NIST standards and audit controls)

Attachment B:	Date Sent: Friday, October 25, 2013	Date Due: Friday, November 8, 2013
----------------------	--	---

OMB Memo: Safeguarding Personally Identifiable Information, M-06-15, May 22, 2006

Attachment D:	Date Sent: Tuesday, October 29, 2013	Date Due: Tuesday, November 12, 2013
----------------------	---	---

OMB Memo: Protection of Sensitive Agency Information, M-06-16, June 23, 2006

Attachment E:	Date Sent: Wednesday, October 30, 2013	Date Due: Wednesday, November 13, 2013
----------------------	---	---

OMB Memo: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, M-06-19, July 12, 2006

Attachment F:	Date Sent: Thursday, October 31, 2013	Date Due: Thursday, November 14, 2013
----------------------	--	--

OMB Memo: Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

Attachment G:	Date Sent: Friday, November 1, 2013	Date Due: Friday, November 15, 2013
----------------------	--	--

President's Identity Theft Task Force: Combating Identity Theft - A Strategic Plan, April 11, 2007

Attachment H:	Date Sent: Tuesday, November 5, 2013	Date Due: Tuesday, November 19, 2013
----------------------	---	---

OMB Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16, May 22, 2007

Attachment I:	Date Sent: Wednesday, November 6, 2013	Date Due: Wednesday, November 20, 2013
----------------------	---	---

Critical Security Controls for Effective Information Security

Federal Legislation:

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) Issued in 2009

From VA's website - http://www.va.gov/about_va/va_notices.asp:

HITECH ACT Press Releases

"Announcements provided by VA in compliance with the HITECH Act of 2009. Please call VA's resource line 1-800-983-0931 for additional information or view more content related to the HITECH ACT here."

We called VA's resource line and got the following message:

"Thank you for calling the VA health resource center. This is a temporary greeting to let you know that you have successfully reached a number at the HRC. The routing will be activated when authorized. Goodbye and thank you for calling."

1. Do you anticipate activating the VA Health Resource Center number in the near future? Yes No
Other:
 - a. If yes, please provide the date of activation and the reason why it was not activated earlier. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, memorandums)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

2. As stated on the VA website, please provide the Subcommittee with the announcements showing VA's compliance with the HITECH Act of 2009.
 - a. Documentation available (i.e. policy, guidelines, actual announcements, other compliance related documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

"(a) ESTABLISHMENT.—There is established **within the Department of Health and Human Services an Office of the National Coordinator for Health Information Technology** (referred to in this section as the 'Office'). The Office shall be headed by a **National Coordinator** who shall be appointed by the Secretary and shall report directly to the Secretary.

"(1) ensures that **each patient's health information is secure and protected**, in accordance with applicable law;

"(2) HIT POLICY COORDINATION.—

"(A) IN GENERAL.—The National Coordinator **shall coordinate health information technology policy and programs of the Department with those of other relevant executive branch agencies** with a goal of avoiding duplication of efforts and of helping to ensure that each agency undertakes health information technology activities primarily within the areas of its greatest expertise and technical capability and in a manner **towards a coordinated national goal**.

3. Please describe the types of coordination and other interactions that occur between VA and OIT, if any. [Click here to enter text.](#)
 - a. Documentation available (i.e. policy, guidelines, reports)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

There is established a **HIT Policy Committee** to make policy recommendations to the National Coordinator relating to the **implementation of a nationwide health information technology infrastructure**, including implementation of the strategic plan described in section 3001(c)(3).

- 4. Does VA coordinate and provide input to the HIT Policy Committee? Yes No Other:
 - a. If yes, in what capacity? If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, actual documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

- 5. Does VA participate or utilize any of the following activities within the HIT Policy Committee:
 - a. Membership on the Committee? Yes No Other:
 - b. Membership on any of the Workgroups? Yes No Other:
 - c. Address or incorporate any of their recommendations? Yes No Other:
 - d. Provide any input on the Committee's recommendations? Yes No Other:
 - e. For each, if yes, please provide additional detail. For each, if no, please explain why not:
 - f. Documentation available (i.e. policy, guidelines, other evidential material)? Yes No Other:
 - g. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

“(a) ESTABLISHMENT.—There is established a committee to be known as the **HIT Standards Committee** to recommend to the National Coordinator **standards, implementation specifications, and certification criteria for the electronic exchange and use of health information** for purposes of adoption under section 3004, consistent with the implementation of the strategic plan described in section 3001(c)(3) and beginning with the areas listed in section 3002(b)(2)(B) in accordance with policies developed by the HIT Policy Committee.

- 6. Does VA coordinate and provide input to the HIT Standards Committee? Yes No Other:
 - a. If yes, in what capacity? If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, actual documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

- 7. Does VA participate or utilize any of the following activities offered by the HIT Standards Committee:
 - a. Membership on the Committee? Yes No Other:
 - b. Membership on any of the Workgroups? Yes No Other:
 - c. Address or incorporate any of their recommendations? Yes No Other:
 - d. Provide any input on the Committee's recommendations? Yes No Other:
 - e. For each, if yes, please provide additional detail. For each, if no, please explain why not:
 - f. Documentation available (i.e. policy, guidelines, other evidential material)? Yes No Other:
 - g. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

- 8. Does VA provide any input to the Committee's standards on electronic exchange and use of health information? Yes No Other:
 - a. If yes, please provide additional details. If no, please explain why not:
 - b. Does VA incorporate these standards for their electronic exchange and use of health information? Yes No Other:
 - c. If yes, please provide additional details. If no, please explain why not:

- d. Documentation available (i.e. policy, guidelines, actual standards, other evidential material)? Yes No Other:
- e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
9. Does VA provide any input to the Committee's implementation specifications for the electronic exchange and use of health information? Yes No Other:
- a. If yes, please provide additional details. If no, please explain why not:
- b. Does VA incorporate these implementation specifications for their electronic exchange and use of health information? Yes No Other:
- c. If yes, please provide additional details. If no, please explain why not:
- d. Documentation available (i.e. policy, guidelines, actual specifications, other evidential material)? Yes No Other:
- e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
10. Does VA provide any input to the Committee's certification criteria for the electronic exchange and use of health information? Yes No Other:
- a. If yes, please provide additional details. If no, please explain why not:
- b. Does VA incorporate the Committee's certification criteria for their electronic exchange and use of health information? Yes No Other:
- c. If yes, please provide additional details. If no, please explain why not:
- d. Documentation available (i.e. policy, guidelines, actual specifications, other evidential material)? Yes No Other:
- e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

“(3) STRATEGIC PLAN.—

“(A) IN GENERAL.—The National Coordinator shall, in consultation with other **appropriate Federal agencies** (including the National Institute of Standards and Technology), update the **Federal Health IT Strategic Plan** (developed as of June 3, 2008) to include **specific objectives, milestones, and metrics** with respect to the following:

11. Has VA consulted with and/or provided input to OIT's Federal Health IT Strategic Plan? Yes No Other:
- a. If yes, please provide additional detail. If no, please explain why not:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
12. Has VA implemented any specific objectives from the Federal Health IT Strategic Plan? Yes No Other:
- a. If yes, please describe the objectives that were implemented. If no, please explain why not:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
13. Has VA incorporated any milestones from the Federal Health IT Strategic Plan? Yes No Other:
- a. If yes, please describe the milestones that were incorporated. If no, please explain why not:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

14. Has VA utilized any metrics from the Federal Health IT Strategic Plan? Yes No Other:
- If yes, please describe the metrics that were utilized. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

“(1) Health information technology architecture that will support the **nationwide electronic exchange and use of health information** in a secure, private, and accurate manner, including connecting health information exchanges, and which may include updating and implementing the infrastructure necessary within different agencies of the Department of Health and Human Services to support the electronic use and exchange of health information.

15. Has VA consulted with and/or provided input to OIT’s Health information technology architecture to support the electronic use and exchange of health information? Yes No Other:
- If yes, please provide additional detail. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, VA’s health IT architecture, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
16. Does VA utilize OIT’s Health IT architecture to assist in their exchange of health information with DOD? Yes No Other:
- If yes, please provide additional detail. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
17. Does VA's enterprise architecture incorporate any of the HIT architecture, in terms of data, security, technology, performance, business etc.? Yes No Other:
- If yes, please provide additional detail. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, EA documents, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
18. Does VA's Veterans Health Information Systems and Technology Architecture (Vista) incorporate any of the HIT architecture, in terms of data, security, technology, performance, business etc.? Yes No Other:
- If yes, please provide additional detail and the relationship between the two. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, EA documents, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

HEALTH INFORMATION TECHNOLOGY EXTENSION PROGRAM.—

To assist health care providers to adopt, implement, and effectively use certified EHR technology that allows for the electronic exchange and use of health information, the Secretary, acting through the Office of the National Coordinator, shall establish a health information technology extension program to provide health information technology assistance services to be carried out through the Department of Health and Human Services. The National Coordinator shall **consult with other Federal agencies with demonstrated experience and expertise in information technology services**

19. Does VA utilize OIT's Health Information Technology Extension Program to adopt, implement, and effectively use certified EHR technology? Yes No Other:
- If yes, please provide additional detail on how it is utilized. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
20. Does VA consult with OIT's National Coordinator to share experiences and expertise within information technology services? Yes No Other:
- If yes, please provide additional detail. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

HEALTH INFORMATION TECHNOLOGY RESEARCH CENTER.—

“(1) IN GENERAL.—The Secretary shall create a **Health Information Technology Research Center** (in this section referred to as the ‘Center’) to provide **technical assistance and develop or recognize best practices** to support and accelerate efforts to adopt, implement, and effectively utilize health information technology that allows for the electronic exchange and use of information in compliance with standards, implementation specifications, and certification criteria adopted under section 3004. **The Center shall incorporate input from—**

“(A) other Federal agencies with demonstrated experience and expertise in information technology services

21. Does VA utilize OIT's Health Information Technology Research Center to provide health information technology technical assistance and develop best practices? Yes No Other:
- If yes, please provide additional detail on how it is utilized. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
22. Has VA consulted with and/or provided input to OIT's Health Information Technology Research Center to support the electronic use and exchange of health information? Yes No Other:
- If yes, please provide additional detail. If no, please explain why not:
 - Has VA provided the Center with any best practices? Yes No Other:
 - Documentation available for ‘a’ and ‘b’ (i.e. policy, guidelines, VA's best practices, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
23. Does VA consult with OIT's Health Information Technology Research Center to share experiences and expertise within information technology services? Yes No Other:
- If yes, please provide additional detail. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

The HITECH Act requires HIPAA covered entities to report data breaches affecting 500 or more individuals to HHS and the media, in addition to notifying the affected individuals.

a) IN GENERAL.—A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, **in the case of a breach** of such information that is discovered by the covered entity, **notify each individual whose unsecured protected health information has been**, or is reasonably believed by the covered entity to have been, **accessed, acquired, or disclosed** as a result of such breach.

(d) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and **in no case later than 60 calendar days after the discovery of a breach** by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

24. Since January 2010, on how many occasions did VA have their data breached? [Click here to enter text.](#)
- a. How many of these breaches affected 500 or more individuals? [Click here to enter text.](#)
 - a. Of these breaches, on how many occasions has VA reported a data breach affecting 500 or more individuals? [Click here to enter text.](#)
 - b. For each, please provide additional background information.
 - c. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
 - b. For each, please provide additional background information.
 - c. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
25. Since January 2010, in instances where VA has found a data breach affecting 500 or more individuals, did VA report them to:
- a. HHS? Yes No Other:
 - b. The media? Yes No Other:
 - c. The affected individuals? Yes No Other:
 - d. For each, if yes, please provide additional detail on how these reports are issued. For each, if no, please explain why not:
 - e. Documentation available (i.e. policy, guidelines, actual reports to HHS, the media, affected individuals, other evidentiary documents)? Yes No Other:
 - f. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
26. Since January 2010, in instances where VA has found a data breach affecting 500 or more individuals, did VA report them within 60 calendar days to:
- a. HHS? Yes No Other:
 - b. The media? Yes No Other:
 - c. The affected individuals? Yes No Other:
 - d. For each, if yes, please provide additional detail and dates. For each, if no, please explain why not:
 - e. Documentation available (i.e. policy, guidelines, actual reports with dates to HHS, the media, affected individuals, other evidentiary documents)? Yes No Other:
 - f. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

2) **BURDEN OF PROOF.**—The covered entity involved (or business associate involved in the case of a notification required under subsection (b)), shall have the burden of **demonstrating that all notifications were made** as required under this part, including **evidence demonstrating the necessity of any delay.**

27. Does VA have a burden of proof demonstrating that for each data breach all notifications were made to HHS, the media, and the affected individuals, including demonstrating the necessity of any delay? Yes No Other:
- a. If yes, please provide additional detail on this process. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, burden of proof, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

(e) METHODS OF NOTICE.—

(1) **INDIVIDUAL NOTICE.**—Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

(A) **Written notification** by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

Also through **electronic notification** to the individual, a substitute form of notice shall be provided, may provide information to individuals by **telephone or other means**, as appropriate

28. Since January 2010, with respect to a breach, how has VA communicated with the affected individual? Please describe in detail each method of notice. [Click here to enter text.](#)
- a. Documentation available (i.e. policies, guidelines, methods of notice via mail, email etc., other actual evidentiary documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

(2) **MEDIA NOTICE.**—Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach

29. Since January 2010, with respect to a breach, how has VA communicated with media outlets? Please describe in detail each method of notice. [Click here to enter text.](#)
- a. Documentation available (i.e. policies, guidelines, methods of notice via mail, email etc., other actual evidentiary documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

4) **POSTING ON HHS PUBLIC WEBSITE.**—The Secretary shall make available to the public on the Internet website of the **Department of Health and Human Services** a list that identifies each covered entity involved in a breach described in subsection (a) in which the **unsecured protected health information of more than 500 individuals is acquired or disclosed.**

30. Has VA provided HHS a list that identifies each covered entity involved in a breach where unsecured protected health information of more than 500 individuals was compromised? Yes No Other:

- a. If yes, please describe the interaction and coordination between VA and HHS. If no, please explain why not:
- b. Were VA's list and information made publicly available to the HHS website? Yes No Other:
- c. If yes, please describe additional detail on this process. If no, please explain why not:
- d. Documentation available for 'a' and 'b' (i.e. policy, guidelines, VA's list to HHS, website url's, actual evidentiary documents)? Yes No Other:
- e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

HITECH Act Legislative Requirement:

f) **CONTENT OF NOTIFICATION** .—Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:

- (1) A brief description of **what happened**, including the date of the breach and the date of the discovery of the breach, if known.
- (2) A description of **the types of unsecured protected health information that were involved** in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
- (3) The **steps individuals should take to protect themselves** from potential harm resulting from the breach.
- (4) A brief description of **what the covered entity involved is doing to investigate the breach**, to mitigate losses, and to protect against any further breaches.
- (5) **Contact procedures for individuals to ask questions** or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

31. For each notice of breach, does VA include the following attributes:
- a. Description of what happened? Yes No Other:
 - a. Date of the breach? Yes No Other:
 - b. Discovery of the breach? Yes No Other:
 - b. Description of the types of unsecured protected health information? Yes No Other:
 - a. Full name? Yes No Other:
 - b. Social Security number? Yes No Other:
 - c. Date of birth? Yes No Other:
 - d. Home address? Yes No Other:
 - e. Account number? Yes No Other:
 - f. Disability code? Yes No Other:
 - c. Steps individuals should take to protect themselves from potential harm resulting from the breach? Yes No Other:
 - d. Description of what VA is doing to investigate the breach? Yes No Other:
 - a. To mitigate losses? Yes No Other:
 - b. To protect against any further breaches? Yes No Other:
 - e. Contact procedures for individuals to ask questions or learn additional information? Yes No Other:
 - a. Toll-free telephone number? Yes No Other:
 - b. E-mail address? Yes No Other:
 - c. Web site? Yes No Other:
 - d. Postal address? Yes No Other:
 - f. Documentation available for 'a' - 'e' (i.e. policy, guidelines, notice of breach, actual evidentiary documents)? Yes No Other:
 - g. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

The Subcommittee would like to thank VA for taking the time to answer our questions. In case we have additional questions, for each attachment, provide a point of contact(s) or person(s) responsible for filling out the above. If you have any questions, please contact Ashfaq Huda, 202.225.6624, ashfaq.huda@mail.house.gov. Please return your responses along with all supporting documentation required to verify the satisfaction of our questions by **Monday, November 11, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment C** and associated documents can be submitted via email to Ashfaq, or you may send it via cd to the following address:

Ashfaq Huda
Senior Professional Staff Member
Subcommittee on Oversight and Investigations
House Committee on Veterans' Affairs
335 Cannon House Office Building
Washington, D.C. 20515
