OFFICE OF RESEARCH OVERSIGHT
Examples and a Brief Guide for Reporting
Apparently Serious Research Information Security Problems
That May Be Reportable to ORO under VHA Handbook 1058.01

September 14, 2015

VHA Handbook 1058.01: Research Compliance Reporting Requirements

§4.t. Serious Problem. A serious problem is a problem in human research or research information security that may reasonably be regarded as:

(1) Presenting a genuine risk of substantive harm, to the safety, rights, or welfare of human research subjects, research personnel, or others, including their rights to privacy and confidentiality of identifiable private information; or

(2) Substantively compromising a facility’s HRPP [Human Research Protection Program] or research information security program.

§10.a. Notification Requirements. VA personnel, including WOC and IPA appointees, must ensure notification of the ACOS/R&D, Information Security Officer (ISO), Privacy Officer (PO), and relevant investigators immediately (i.e., within one hour) upon becoming aware of any information security incidents related to VA research, including any inappropriate access, loss, or theft of PHI; noncompliant storage, transmission, removal, or destruction of PHI; or theft, loss, or noncompliant destruction of equipment containing PHI.

IMPORTANT NOTE: It is the role and responsibility of the relevant research review committee(s) [i.e., Institutional Review Board (IRB), Institutional Animal Care and Use Committee (IACUC), Subcommittee on Research Safety (SRS), and/or Research and Development Committee (R&DC)] to determine whether a particular situation actually constitutes a serious research information security problem. However, VA personnel are required to report any situation that appears to represent a serious research information security problem. Examples are provided here to assist in identifying such problems, but the examples should be not considered either exhaustive or definitive. ORO strongly recommends that research review committees clearly document case-specific determinations and justifications related to their evaluations of apparently serious research information security problems.

A. Examples of Apparently Serious Problems in Research Information Security That May Be Reportable to ORO under VHA Handbook 1058.01 §10.a:

(1) Inappropriate access, loss, or theft of protected health information (PHI); noncompliant storage, transmission, removal, or destruction of PHI; or theft, loss, or noncompliant destruction of equipment containing PHI. Issues for the research review committee to consider in evaluating any information security incident may include the following:

a. What level of subject identification was contained in the pertinent PHI (e.g., name, SSN, address, phone number)?
b. How sensitive and specific was the pertinent PHI (e.g., HIV diagnosis, alcohol/drug dependence)?
c. What is the likelihood of a permanent loss versus temporary displacement?
d. What is the likelihood of actual unauthorized access?
e. Who and how many (other Veterans, researchers, sponsors, etc.) accessed the PHI?
f. How many documents, individual subject records, and/or pieces of equipment were accessed/lost/stolen/stored/transmitted/removed/destroyed in this one incident?
g. Is this a repeated instance of noncompliance (same type, investigator, research group)?
(2) Unauthorized destruction (accidentally or intentionally) of research documents or records. *Additional* issues for the research review committee to consider may include the following:
   a. Was the sole copy of the record destroyed?
   b. How many records were destroyed in this one incident?
   c. Is the National Archives and Records Administration (NARA) required to be notified?

(3) Loss, theft, or unauthorized destruction of equipment (e.g., laptops, other mobile devices, external storage media) containing VA research-related PHI. *Additional* issues for the research review committee to consider may include the following:
   a. Was the equipment encrypted according to VA standards?
   b. Did the equipment contain the only copy of the research record?

(4) Transmission of VA research-related PHI not encrypted according to VA standards. *Additional* issues for the research review committee to consider may include the following:
   a. Was the PHI transmitted outside of VA?
   b. Was the PHI transmitted to its intended (authorized) recipient?
   c. Was the PHI encrypted, but not according to VA standards?

(5) Use or connection of unauthorized equipment (e.g., non-VA thumb drive, unauthorized personally owned equipment) to store, process, or transmit VA research-related PHI. *Additional* issues for the research review committee to consider may include the following:
   a. Was the equipment connected to the VA network?
   b. Was the equipment subsequently taken outside of the VA facility or connected to non-VA information systems?

(6) Malicious attack on or unauthorized access to VA information system containing VA research-related PHI. *Additional* issues for the research review committee to consider may include the following:
   a. Was VA PHI compromised or potentially compromised (confidentiality, integrity, and/or availability of the system affected)?
   b. Was the attack/access isolated or widespread?

---

1 For detailed requirements related to human research problems, see VHA Handbook 1058.01 §6.c. and ORO Decision Chart “Reporting Local Death, Local Serious Adverse Events (SAEs), and Serious Problems in VA Research” (Revised September 14, 2015). Examples of apparently serious problems in human research that may be reportable to ORO include the following:
   (1) Any situation that requires action to prevent an immediate hazard to subjects or others.
   (2) Any serious research-related injury to human research subjects, research personnel, or others.
   (3) Any problem described in a VA Pharmacy Benefits Management alert relevant to local human subjects.
   (4) Any problem described in a Data Monitoring Committee report.
   (5) Any combination of problems that collectively present a genuine risk of substantive harm to the safety, rights, or welfare of human research subjects, research personnel, or others, or substantively compromise a facility’s HRPP.
B. Brief Guide for Reporting Apparently Serious Information Security Problems in VA Research. For detailed requirements, see VHA Handbook 1058.01 §10.

A VA employee becomes aware of an apparently SERIOUS INFORMATION SECURITY PROBLEM in VA research.

- The employee must ensure IMMEDIATE NOTIFICATION (with 1 hour) of the ACOS/R&D, the Information Security Officer (ISO), the Privacy Officer (PO), and any relevant investigators.

- If the immediate notification was not in writing, the employee must also ensure written notification of the ACOS/R&D within 5 business days.

- If the incident results in an Issue Brief sent to VHACO, an individual breach notification, the provision of credit monitoring, a HITECH breach notification, or notification to/from OIG, the Facility Director must report the incident to ORO within 5 business days after the action.

- If VA records were destroyed, the ACOS/R&D must IMMEDIATELY notify the Records Management official.
- The ACOS/R&D must also IMMEDIATELY notify any relevant research review committees.
- If the problem also involves human research, see Footnote 1 on page 2.

- Each relevant research review committee must review the incident at its next convened meeting within 30 business days.
- The committee must determine and document whether a serious problem occurred and whether/what remedial actions are warranted.
- If a serious problem occurred, the committee must notify the Facility Director and the ACOS/R&D within 5 business days after its determination.

- The Facility Director must report the serious problem to ORO within 5 business days after receiving the notification.

- If the research review committee makes additional determinations under its authority, reporting requirements pertinent to those determinations must also be satisfied.
- Additional reporting may be required under local SOPs or by external agencies or sponsors. If in doubt, check with the relevant entities.