OFFICE OF RESEARCH OVERSIGHT

Possible Examples of Serious Problems and Serious Noncompliance In Human Research and Research Information Security under VHA Handbook 1058.01

NOTE: *Only the IRB can determine whether a particular situation actually constitutes a serious problem or serious noncompliance. However, ORO strongly recommends that IRBs clearly document case-specific justifications when an event listed here is determined not to have been so.*

A. VHA Handbook 1058.01 §4t. 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 or research information security program.*

Examples of Possibly Reportable Serious Problems in Human Research:

(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.

Examples of Possibly Reportable Serious Problems in Research Information Security:

(1) Inappropriate access, loss, or theft of documents containing PHI (e.g., informed consent forms, HIPAA authorization forms, case report forms). Issues for the research review committee to consider in evaluating the incident may include the following:
    a. What is the likelihood of a permanent loss versus temporary displacement?
    b. What is the likelihood of actual unauthorized access?
    c. Who accessed the PHI (other Veterans, researchers, sponsors, etc.) and how many?
    d. How many documents were lost/stolen/accessed in this one incident?
    e. What level of subject identification was contained in the document(s) (e.g., name, SSN, address, phone number)?
    f. How sensitive and specific was the health information in the document(s) (e.g., HIV diagnosis, alcohol/drug dependence)?
    g. Is this a repeated instance of noncompliance (same type, investigator, research group)?
(2) Unauthorized destruction (accidentally or intentionally) of research records. Issues for the research review committee to consider in evaluating the incident 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. Issues for the research review committee to consider in evaluating the incident 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?
    c. What was the extent of the PHI contained on the equipment?
(4) Transmission of VA research-related PHI not encrypted according to VA standards. Issues for the research review committee to consider in evaluating the incident 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. Issues for the research review committee to consider in evaluating the incident 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. Issues for the research review committee to consider in evaluating the incident may include the following:
   a. Was VA PHI compromised or potentially compromised (confidentiality, integrity, and/or availability affected)?
   b. Was the attack/access isolated or widespread?

B. VHA Handbook 1058.01 §4s. Serious Noncompliance. *Serious noncompliance is any failure to adhere to requirements for conducting* ***human research*** *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.

Examples of Possibly Reportable Serious Noncompliance in Human Research

(1) Initiation of human research without required IRB approval.
(2) Initiation of human research without R&D Committee approval.
(3) Initiation of human research without ACOS/R notification that the research may begin.
(4) Failure to obtain informed consent for one or more subjects (where required, unless waived by the IRB).
(5) Failure to obtain HIPAA authorization for one or more subjects (where required, unless waived by the IRB).
(6) Modification of a protocol without IRB approval (except to prevent immediate hazards to subjects).
(7) Failure to notify the IRB of a death, SAE, or problem as required.
(8) Unfounded labeling of a death, SAE, or problem as "anticipated" or "not related" to the research.
(9) Conduct of research without required credentialing, privileging, or initial training.
(10) Conduct of research involving women known to be pregnant, prisoners, or children, or of international research, without required approvals from the Facility Director or Chief Research and Development Officer, as applicable.
(11) Failure to implement, in a timely fashion, any protocol or informed consent modifications, or other changes required by the IRB.
(12) Failure to remediate any noncompliance in a timely fashion as required by the IRB.
(13) Continuation of human research beyond the specified IRB approval period (except where in subjects' best interests as determined by the IRB Chair).
(14) Substantive informed consent or HIPAA authorization deficiencies.
(15) Failure to obtain documentation of informed consent (where required, unless waived by the IRB).
(16) Substantive deviations from IRB-approved protocols, including substantive violations of inclusion or exclusion criteria.
(17) Any finding by any entity, including clinical trial monitors, of apparent serious noncompliance as listed here.
(18) Programmatic noncompliance (e.g., violation of IRB quorum requirements; improper approval or documentation of exemptions or waivers; failure to ensure review of proposed research sufficient to identify and address privacy or data security concerns).
(19) Any combination of noncompliant actions 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.