

OFFICE OF RESEARCH OVERSIGHT
GUIDANCE ON REPORTING DEFICIENT HIPAA AUTHORIZATIONS
(Original date June 22, 2016; Revised March 10, 2021)

The Office of Research Oversight (ORO) has received a variety of questions related to the requirements for reporting deficient Health Insurance Portability and Accountability Act (HIPAA) authorizations, including (i) the validity of authorizations lacking the date of the research subject's signature; (ii) actions to be taken if Protected Health Information (PHI) was used or disclosed pursuant to an invalid authorization; and (iii) whether all HIPAA authorization deficiencies must be reported to the Institutional Review Board (IRB) within 5 business days as apparent serious or continuing noncompliance under VHA Directive 1058.01 §7.c.

ORO provides the following guidance on reporting requirements for deficient HIPAA authorizations.

1. VHA Directive 1605.1 §§14.b&c specify that a valid HIPAA authorization must contain certain essential elements (including the "signature of the individual ... and date signed"). HIPAA authorizations missing any of these essential elements are considered invalid for research and would not constitute valid legal authority for use or disclosure of the individual's PHI without a waiver of HIPAA authorization.
2. The VHA Privacy Office, which establishes and interprets HIPAA Privacy Rule requirements for VHA, has indicated that the HIPAA authorization must be dated at the time the individual or personal representative providing the authorization signs the form in order for the HIPAA authorization to be valid. VA Form 10-0493 (*Authorization for Use and Release of Individually Identifiable Health Information Collected for VHA Research*) is currently required when used as a standalone document by VA researchers, i.e., not combined with the research informed consent document. The signature date cannot be added later by investigators to "validate" an undated HIPAA authorization.
3. When PHI has been used or disclosed without legal authority as a result of an invalid HIPAA authorization, further uses or disclosures must not occur until the legal authority to do so is established. For example, if a subject signs the HIPAA authorization but forgets to include the signature date, remediation to establish legal authority for use and disclosure of the subject's PHI would require that:
 - (a) The subject later add and initial the date on the original authorization form; or
 - (b) The subject sign and date a new authorization form; or
 - (c) The IRB approve a waiver of authorization (for example, where (a) and (b) are not practicable because the investigator is unable to locate the individual or the individual is deceased and the additional applicable criteria at VHA Directive 1200.05 §23.b are fully satisfied and documented).
4. ORO guidance specifies that "substantive" deficiencies in HIPAA authorizations constitute an example of apparently serious noncompliance that must be reported to the IRB within 5 business days ("Examples of Noncompliance in VA Human Subjects Research that ORO Typically Considers to Meet the Definition of Serious or Continuing Noncompliance under VHA Directive 1058.01," March 8, 2021).
5. IRBs may develop Standard Operating Procedures (SOPs) to define "substantive" deficiencies in HIPAA authorizations that must be reported as apparent serious noncompliance. For example, IRBs may define in their SOPs whether omission of the signature date on a single subject's

OFFICE OF RESEARCH OVERSIGHT
GUIDANCE ON REPORTING DEFICIENT HIPAA AUTHORIZATIONS
(Original date June 22, 2016; Revised March 10, 2021)

signed HIPAA authorization, which is promptly remediated upon discovery, should be considered apparent serious noncompliance that must be reported to the IRB within 5 business days.

6. Similarly, IRBs may develop SOPs to define when a noncompliant use or disclosure of PHI must be reported as apparent serious noncompliance. For example, IRBs may define in their SOPs whether the inclusion in a VA research data set of a single individual's PHI under a signed but invalid HIPAA authorization, where that individual's data are promptly removed from the data set upon discovery, should be considered apparent serious noncompliance that must be reported to the IRB within 5 business days.
7. Regardless of whether reporting to the IRB is required, however, if the investigator has accessed, used, or collected an individual's PHI without a "valid" HIPAA authorization, the deficiency must still be reported to the facility Privacy Officer as a privacy incident, even where the deficiency has been promptly remediated.
8. In determining whether or not any apparent serious or continuing noncompliance incident related to HIPAA authorization actually constitutes serious or continuing noncompliance, IRBs should consider factors such as (i) whether the deficiency has been, or will be, promptly remediated; (ii) whether the deficiency resulted in noncompliant uses or disclosures of PHI; (iii) the number of research subjects affected; and (iv) the nature and degree of any harm to subjects (including harm to privacy). IRBs may develop SOPs to operationalize "serious or continuing noncompliance" (consistent with the definitions at VHA Directive 1058.01 §§3.c&o) for use in their determinations.
9. If an IRB receives periodic compliance audit findings indicating that deficient HIPAA authorizations have been identified, the IRB should establish and consistently employ procedures for reviewing those reports and documenting case-specific IRB determinations, justifications, and required remedial actions, if any.

In sum, there are several issues to consider related to deficient HIPAA authorizations, including: (i) the validity of the deficient authorization; (ii) whether the deficient authorization actually resulted in the use or disclosure of PHI without legal authority; (iii) remediation of the deficiency; and (iv) whether the deficiency must be reported to the IRB within 5 business days because it constitutes apparent serious or continuing noncompliance as generally described under VHA Directive 1058.01 §7.c, and as further defined under specific situations per local SOPs.

However, regardless of whether a HIPAA authorization deficiency constitutes serious or continuing noncompliance that must be reported under VHA Directive 1058.01 and local SOPs, no authorization that is invalid can be used as legal authority for the use or disclosure of PHI. Such invalid use or disclosure must be reported to the Privacy Officer and addressed to ensure that a valid authorization (or waiver thereof, if justified, approved and documented) is in place before any future uses or disclosures are made.