
Section 1: GENERAL PRIVACY RULES

1.2 Privacy Compliance Policies

PURPOSE

To describe the HIPAA Enforcement Rule provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

POLICY

1. Application: The University of Florida (UF) will endeavor to abide by current and applicable health information privacy and security laws, regulations and rules, as appropriate and as required by both federal and state agencies, including but not limited to, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), modified by the Genetic Information Nondiscrimination Act of 2008 (GINA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).
2. Non-retaliation: UF may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for:
 - a. Filing an information privacy or security complaint;
 - b. Testifying, assisting, or participating in a privacy investigation, compliance review, proceeding, or hearing; or
 - c. Opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Rule.
3. The Privacy Office shall:
 - a. Provide copies of records and compliance reports as may be necessary to enable the Secretary to ascertain whether UF has complied or is complying with the applicable Privacy Rules.
 - b. Cooperate with complaint investigations and compliance reviews, if the Secretary undertakes an investigation or compliance review of UF's policies, procedures, or practices.
 - c. Permit access to information: by the Secretary during normal business hours to UF's facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable Privacy Rule provisions.

DEFINITIONS

Administrative Simplification Provision - means any requirement or prohibition established by:

- 42 U.S.C. 1320d–1320d–4, 1320d– 7, 1320d–8, and 1320d–9;
- Section 264 of Pub. L. 104–191;
- Sections 13400–13424 of Public Law 111–5; or
- 45 CFR Parts 160 - 164.

PRIVACY REQUIREMENTS

1. **Applicability:** The standards, requirements, and implementation specifications adopted under the federally mandated Privacy and Security Rules, apply to a Health Care Provider who transmits any protected health information (PHI) in electronic form in connection with a transaction covered by the Privacy Rule.
2. **Compliance Dates:** Compliance dates for implementation of new or modified standards and implementation specifications of federal rules, unless otherwise specified, are generally no later than 180 days from the effective date.
3. **Preemption of State Law:**
 - a. A standard, requirement, or implementation specification adopted under [the privacy regulations] that is contrary to a provision of State law preempts the provision of State law, except one or more of the following conditions is met:
 - b. A determination is made by the Secretary... that the provision of State law is necessary;
 - c. The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under [the privacy regulations];
 - d. The provision of State law... provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
 - e. The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

NOTE: UF has adopted the findings of the Florida State Law preemption analysis provided by the American Hospital Association.

4. **Principles for Achieving Compliance:**
 - a. The Secretary will seek the cooperation of covered entities (CEs) and business associations (BAs) in obtaining compliance with the requirements of the applicable administrative simplification provisions.
 - b. The Secretary may provide technical assistance to CEs and BAs to help them comply voluntarily with the applicable administrative simplification provisions.
5. **Complaints to the Secretary:**
 - a. A person who believes a CE or BA is not complying with the requirements of the administrative simplification provisions may file a complaint with the Secretary of Health and Human Services.
 - b. Requirements for filing complaints:
 - i. A complaint must be filed in writing, either on paper or electronically.
 - ii. A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s)
 - iii. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
 - iv. The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

6. Investigation of complaints:

- a. The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.
- b. The Secretary may investigate any other complaint filed under this section.
- c. An investigation under this section may include a review of the pertinent policies, procedures, or practices of the CE or BA and of the circumstances regarding any alleged violation.
- d. At the time of the initial written communication with the CE or BA about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

7. Compliance Reviews:

- a. The Secretary will conduct a compliance review to determine whether a CE or BA is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.
- b. The Secretary may conduct a compliance review to determine whether a CE or BA is complying with the applicable administrative simplification provisions in any other circumstance.
- c. PHI obtained by the Secretary in connection with an investigation or compliance review will not be disclosed, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

8. Responsibilities of Covered Entities and Business Associates:

- a. Provide records and compliance reports. A CE or BA must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the CE or BA has complied or is complying with the applicable administrative simplification provisions.
- b. Cooperate with complaint investigations and compliance reviews. A CE or BA must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices to determine whether it is complying with the applicable administrative simplification provisions.
- c. Permit access to information. A CE or BA must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions.

9. Resolution Where Noncompliance Is Indicated:

- a. If an investigation of a complaint or a compliance review indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.
- b. If the matter is resolved by informal means, the Secretary will so inform the CE or BA and, if the matter arose from a complaint, the complainant, in writing.
- c. If the matter is not resolved by informal means, the Secretary will:
 - i. So inform the CE or BA and provide an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration. The CE or BA must submit any such evidence to the Secretary within 30 days of receipt of such notification; and

- ii. If, following action pursuant to the paragraph above, the Secretary finds that a civil money penalty should be imposed, inform the CE or BA of such finding in a notice of proposed determination.

10. Resolution When No Violation Is Found:

- a. If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the CE or BA and, if the matter arose from a complaint, the complainant in writing.

REFERENCES

- 1. HIPAA: 45 CFR §160.102 Applicability; §160.201 – 205 Preemption of State Law; §160.300 – 312 Compliance and Investigations; §160.316 Refraining from Intimidation or Retaliation

EXHIBITS

None