Section 1: GENERAL PRIVACY RULES

1.7 Investigating and Responding to Privacy Violations

POLICY

1. Response: The University of Florida (UF) Privacy Office shall:
    a. Review and investigate all privacy-related complaints and reported violations and breaches of information privacy or security, as needed.
    b. Initiate the internal Breach Response Procedure upon confirmation of a breach of PHI that meets the description of this policy.
    c. Assess each event to determine if notification is required.
2. Confidentiality: All investigations and resulting documentation of privacy-related complaints and incidents are strictly confidential and shall not be disclosed to anyone unrelated to an alleged or confirmed violation, unless required by law.
3. Personnel: Privacy analysts appointed by, and under the supervision of, the Chief Privacy Officer will review and determine action on privacy complaints and incidents reported to the UF Privacy Office.
4. Documentation: Investigations, interviews, and determinations regarding privacy-related complaints and incidents will be documented and the documentation will be maintained for at least six (6) years, or longer, if required by law or other circumstances. Documentation will include:
    a. The complaint, preferably provided by the complainant in the complainant's own words, and/or an Incident Report provided by a UF employee;
    b. Detailed descriptions of the findings from reviewing the circumstances of a complaint or incident and interviewing witnesses or other persons with knowledge about the complaint or incident;
    c. A summary of the analyst's determination regarding the validity of the complaint or incident, the outcome of the analyst's investigation, the role of the Privacy Office in the complaint or incident, and, if possible, the root cause(s) of confirmed violations of information privacy or security;
    d. A description of corrective actions recommended, or an explanation of why corrective actions are not needed, and a description of corrective actions actually applied, if different;
    e. A description of risk assessments completed when restricted data is involved;
    f. Any notifications procedures followed, including recommendations and final approvals;
    g. Any mitigation undertaken for each specific reported complaint or incident.
5. Notification: UF will make reasonable efforts to notify persons affected by a confirmed breach of personal information, as required by law.

DEFINITIONS

1. *Investigation:* A formal or systematic examination or research of a privacy complaint or incident.
2. *Mitigation:* To make less severe, to partially remove, or to correct, so that harmful effects of a privacy violation are reduced or eliminated.

3. *Privacy Complaint:* An allegation by an individual that an organization is not complying with the requirements of the federal privacy and/or security regulations or the organization's own policies and procedures related to the privacy / security of personal information.
4. *Privacy Incident:* A known or suspected action, inconsistent with the organization's policies and procedures, or an adverse event, related to restricted data.

PRIVACY REQUIREMENTS

1. A covered entity must document all complaints received, and their disposition, if any.
2. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of the Privacy Rule.
3. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of the Privacy Rule by the covered entity or its business associate.

REFERENCES

1. HIPAA: 45 CFR §164.530 (a) Standard: personnel designations, (c) Standard: safeguards, (d) Standard: complaints to the covered entity, (e) Standard: sanctions, (f) Standard: mitigation

EXHIBITS

None