Section 1: GENERAL PRIVACY RULES

1.8 Breach Notification for Privacy Violations, Appendix B: FIPA

POLICY

1. As required by the Florida Information Protection Act (FIPA), the University of Florida (UF) shall take reasonable measures to protect and secure data in electronic form containing Personal Information.
2. As necessary and appropriate, UF shall take action to mitigate any adverse effect(s) of improper or unauthorized, access, use, or disclosure of Personal Information.
3. Breach Response: Reports and discoveries of breaches of "unsecured" Personal Information will be investigated to determine:
    a. Whether unsecured Personal Information has been, or is reasonably believed by UF to have been accessed, acquired, or disclosed as a result of such breach; and
    b. The degree to which the security or privacy of the Personal Information may have been compromised.
4. The Privacy Office shall:
    a. Receive privacy-related complaints or incidents by telephone, email, fax, or mail.
    b. Register each alleged privacy violation in the online registration/tracking system, which will automatically generate a case-number.
    c. Retain all related documents into the system under the appropriate case-number.
    d. Add notes and other documentation as needed throughout the investigation.

DEFINITIONS

1. ***Breach or Breach of Security (FIPA)***: means unauthorized access of data in *electronic* form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

   Breach does not apply to information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable or information about an individual that has been made publicly available by a federal, state or local government entity.
2. ***FIPA Covered Entity:*** means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. The term includes a governmental entity.
3. ***Personal Information:*** means either of the following:
    a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
        - Social Security number;

- Driver license/identification card number, passport number, military or similar government identification number or document;
- Financial account or credit/debit card number with required security code, access code, or password necessary to permit access to an individual's financial account;
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account

4. ***Notification:*** The act of informing persons affected by a breach of private information that their information was included and steps they can take to protect themselves and their privacy.

5. ***Unsecured Protected Health Information***: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary (of Health and Human Services); specifically, encryption for electronic PHI, and destruction for all other PHI.

PRIVACY REQUIREMENTS

1. Reporting Known or Suspected Breaches

   a. Timely reporting of accurate information by persons who have knowledge that a breach may have occurred is a critical first step in mitigating any breach. Once this information is reported to a single person or department, providing further internal notification to areas that may assist with mitigating the breach is equally important.

   b. Members of the UF's workforce are expected to report known or suspected breaches of information security or patient confidentiality to their supervisor, the IT Security Office, the Privacy Office, or to the UF Privacy Hotline: 1-866-876-4472.

2. Breach Investigations

   a. Upon receipt of a report of a known or suspected breach, the Privacy Office shall initiate a formal investigation, activate the Privacy Incident Response Team (PIRT) as required, manage breach investigations, and maintain all documentation for at least six years.

   b. The Privacy Office shall determine if breach notification under federal or state law is required.

   c. The UF department, division, or unit that was the source of a breach is responsible for costs associated with breach notification (e.g., letter mailings, call center support, etc.).

   d. While each breach investigation is unique, common investigation steps and actions are described below.

      i. Activate PIRT

      ii. Identify and take immediate action to stop the source (e.g., hacking) or the entity responsible for a breach (e.g., workforce member, vendor).

      iii. Identify information systems, applications, or electronic Personal Information involved and begin the identification process for affected individuals.

      iv. Identify the source of individuals involved in the incident.

v. Have UF ISO staff complete a technical forensic analysis, as required, to gather evidence to identify electronic Personal Information compromised.

vi. Identify and sequester pertinent medical records, files, and other documents (paper and electronic).

vii. Determine the need for required breach notification.

3. NOTICE TO DEPARTMENT OF SECURITY BREACH.—

a. Where applicable, UF shall provide notice to the Attorney General, Florida Department of Legal Affairs (Department), of any breach of security affecting 500 or more individuals in this state.

b. Such notice shall be provided as expeditiously as practicable, but no later than **30 days** after the determination of the breach or reason to believe a breach occurred. UF may allow for 15 additional days to provide notice good cause for delay is provided in writing to the Department within 30 days after determination of the breach or reason to believe a breach occurred.

c. Written notice to the department must include:

i. A synopsis of the events surrounding the breach at the time notice is provided.

ii. Number of individuals affected by the breach.

iii. Any services related to the breach being offered or scheduled to be offered, without charge and instructions as to how to use such services.

iv. A copy of the notice to individuals.

v. Name, address, telephone number, and e-mail address for UF contact.

d. If required by the Department, UF shall provide the following additional information:

i. A police report, incident report, or computer forensics report.

ii. A copy of the policies in place regarding breaches.

iii. Steps that have been taken to rectify the breach.

4. NOTICE TO INDIVIDUALS OF SECURITY BREACH.—

a. UF shall give notice to each individual ***in Florida*** whose Personal Information was or reasonably believed to have been, accessed as a result of the breach.

b. Notice shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow UF to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, ***but no later than 30 days after the determination of a breach*** (unless directed by law enforcement or notification provided under HIPAA).

c. UF may delay notification if a law enforcement agency determines that notice to individuals would interfere with a criminal investigation.

d. Notice to affected individuals is not required if, after an appropriate investigation and consultation with relevant law enforcement agencies, UF reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing, maintained for at least 5 years, and provided to the Department within 30 days after the determination.

e. FIPA individual notice exception.

i. Notice provided pursuant to rules, regulations, procedures, or guidelines established by UF's primary or functional federal regulator (i.e., OCR for HIPAA covered entities) is deemed to be in compliance with FIPA's individual notice requirement if UF notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security.

5. Method of Individual Notification

a. Notice to an affected individual shall be by one of the following methods:

i. Written notice sent to the mailing address of the individual or

ii. E-mail notice sent to the e-mail address of the individual in the records of UF.

6. Individual Notification Content

a. Notice to an individual with respect to a breach of security shall include, at a minimum:

i. The date, estimated date, or estimated date range of the breach of security.

ii. A description of the Personal Information involved.

iii. UF contact information.

b. UF may provide substitute notice in lieu of direct notice if the cost of providing notice would exceed $250,000, if affected individuals exceed 500,000 persons, or when UF lacks an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:

i. A conspicuous notice on the UF Privacy Office website and

ii. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

7. NOTICE TO CREDIT REPORTING AGENCIES.

a. UF shall notify, without reasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis if more than 1,000 individuals are notified at a single time.

b. UF shall inform these agencies of the timing, distribution, and content of the notices.

8. NOTICE BY THIRD-PARTY AGENTS

a. In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify UF of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.

b. Upon receiving notice from a third-party agent, UF shall provide notices to the Department and to affected individuals unless another process is dictated by contract with the agent.

REFERENCES

1. Florida Statute: 501.171, Security of confidential personal information
2. UF Regulations: 1.0103 Policies on Restricted Data

EXHIBITS

None