

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

Security: Electronic Databases

A. POLICY

Rev: 06/01/09

1. **Requirements:** Any electronic database containing Protected Health Information (PHI) or Personal Identification Information (PII), maintained by any member of the UF workforce must meet the following conditions:
 - a) *The database must be stored on a secure server, not on a hard drive of any computer, and protected with all security measures required by the IT Security policies and standards, including but not limited to:*
 - (1) Procedures for permitting and authenticating access and terminating access for individuals who are no longer associated with the work for which the database was developed;
 - (2) Processes for logging and periodically monitoring access to the database;
 - (3) Processes for backing up the database files and securely storing the back-ups.
 - b) *Access to the database must be limited:*
 - (1) By password-protected personal accounts assigned to specifically identified individuals who are authenticated by the custodian of the database,
 - (2) To defined work-related purposes and for defined periods of time.
 - c) *A log of individuals who have been given access to the database must be maintained, and should include, at a minimum:*
 - (1) The individual's name and UF Identification number;
 - (2) The date access was given and the reason access was given to the database;
 - (3) The individual's assigned account information, except password;
 - (4) The date access was terminated and the reason for termination.
2. **Products of Electronic Databases:** Paper or hard-copy print-outs or components of electronic databases, which contain PHI or PII, must be stored in lockable, non-portable units, such as filing cabinets, suitable for the format of the database and located in an approved storage area or facility.
3. **Transport of Data:** Any data copied, downloaded, or otherwise moved from the main electronic database onto portable electronic media or devices must be properly encrypted or de-identified.
4. **Purging and Destruction:** The data, including all copies and print-outs of the data, must be properly destroyed when no longer needed. Identifiable personal and patient information may not be removed from UF premises in formats that would allow for easy access by unauthorized persons.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

B. DEFINITIONS

1. **Back-up:** Copy of **electronic** files and applications made to avoid loss of data and facilitate recovery of data and information.
2. **Database:** A collection of information, usually recorded in alpha or numeric terms, and organized for rapid search and retrieval, as by a computer.
3. **Encryption:** The use of an algorithmic process to transform **electronic** data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

C. PRIVACY REQUIREMENTS

1. **Ensure** the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. **Protect** against any reasonably anticipated threats or hazards to the security or integrity of such information, and against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
3. **Implement** policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
4. **Enforce** compliance with the above by its workforce.

D. REFERENCES

1. **HIPAA:** 45 CFR §164.306 (Security standards: General rules), §164.308 (Administrative safeguards).
2. **UF HSC SPICE Policies and Standards:**
http://security.health.ufl.edu/isa_ism/policies.shtml

E. EXHIBITS None