Sample Policies and Procedures for the Use and Disclosure of Protected Health Information (PHI)

POLICY STATEMENT

1. When accessing, using, or disclosing PHI, or when requesting PHI from EUTF, reasonable efforts will be made to limit PHI to the minimum necessary amount to accomplish the intended purpose of the use, disclosure or request.
2. Minimum Necessary Standard refers to divulging the least amount of information possible for a particular use, disclosure, or request.
3. The minimum necessary standard applies to oral, electronic, and written PHI. The minimum necessary standard does not apply to the following uses and disclosures:
    a. to a health care provider for treatment,
    b. to the individual,
    c. made in accordance with a valid authorization,
    d. made to the Secretary of the Dept. of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated,
    e. for which an authorization or opportunity to agree or disagree is not required under the regulation,
    f. that are required for compliance with the general rules under §164.502, and
    g. required for compliance with HIPAA Electronic Data Interchange (EDI) transaction standards.
4. To comply with the minimum necessary standard requirements, the Agency will:
    a. Identify those persons or classes of persons, as appropriate, in the workforce who need access to PHI to carry out their duties;
        i. Identify the categories of PHI to which access is needed and the conditions appropriate to such access.
        ii. Make reasonable efforts to limit the access of its workforce to PHI as described above.
    b. Disclose PHI, as follows:
        i. For routine disclosures made on a recurring basis, the Agency will establish procedures that limit PHI to the amount reasonably necessary to achieve the purpose of the disclosure; and
        ii. Review non-routine requests for disclosure on an individual basis.

PROCEDURES

1. Make reasonable efforts to limit PHI to the minimum necessary standard to accomplish the intended purpose when:
    a. using,
    b. disclosing, and
    c. requesting PHI.
2. If PHI is provided to a contractor, the agency's policies and procedures for handling of PHI must be followed.

3. If there is a breach of PHI (including security breaches), Agency will:
    a. Notify the non-breaching agency in writing no less than twenty calendar days after discovery of the breach
    b. Investigate and report the causes of the breach and any steps that breaching agency will take to mitigate the breach and prevent occurrences
    c. In consultation with non-breaching agency, provide all notifications regarding the breach that breaching agency and/or non-breaching agency are required to make under law
    d. Provide a log of all breaches of unsecured protected health information no later than twenty calendar days after the end of each calendar year.
4. Employees have been divided into categories of permission (or accessibility) to PHI as noted in the chart below. Data security measures designed to protect PHI and limit access to PHI corresponds to the following chart. Individuals who need access to PHI to carry out their daily job duties are identified in the chart below.

Employees with Full Access to PHI	Employees with Limited Access to PHI	Employees with No Access to PHI

Sample Polices and Procedures on Safeguarding Physical, Administrative and Technical PHI

POLICY STATEMENT

Appropriate procedures will be established to physically, administratively, and technically safeguard PHI. Reasonable steps to limit incidental use or disclosure of PHI by anyone other than those individuals specifically authorized to work with PHI will be taken.

PROCEDURES

The following are procedures for safeguarding PHI:

1. Staff with access to PHI are individually responsible for safeguarding PHI in common areas and in their respective workspaces.

2. **Discussion Areas for PHI**: Access to physical areas where PHI is discussed should be limited. Staff are prohibited from discussing PHI in public access areas such as the restroom, hallways, elevator, parking lot/garage, or other public locations.

3. **Storage of PHI:** No document containing PHI will be left out on a desk overnight, unless the desk is in a locked office and the documents with PHI are left face down. When not in immediate use, documents with PHI will be stored in a locked file cabinet. No PHI documents are to be left on copier, fax, and main workspace areas. Any unretrieved documents left on copier, fax, and main workspace areas will be shredded at the end of each business day. Documents containing PHI to be filed are to be sent to on-site storage in a sealed container. Storage boxes are labeled and inventoried. Staff will assure PHI boxes stored are not accessible by anyone other than staff who need access to the information. Electronic (e.g. disc, CD, USB data stick/flash drive) PHI is to be stored encrypted in a locked, fireproof cabinet. Electronic ePHI files will be maintained and stored for six years from the date of creation or the date last in effect (whichever is greater). Documents containing PHI are to be saved on a secure network and not on computer hard drives.

   Because USB devices connect directly into computers (as well as some smart phones) and can store large amounts of data, they can potentially cause serious harm to computers and networks or compromise sensitive data if their use is not properly controlled. Encrypting data that is stored on USB devices is an important step that can prevent a breach if the devices are lost or stolen. Documents containing electronic PHI are not to be stored on USB devices unless required as part of business processes and in an encrypted format.

   No PHI is to be removed from the agency, even on laptop, flash drive or other electronic means.

4. **Computer Access:** The computer security controls include a multi-layered security approach to combine multiple mitigating security controls to protect data, including but not limited to the following:
   a. A password is required to log onto a computer that allows access to PHI.
   b. All staff require their own, individualized clearance and unique user identification.
   c. Passwords must be at least seven (7) characters in length and must be changed once every 120 days.
   d. All passwords should be difficult to guess (e.g., “!H3L1O!” v. “HELLO”). Passwords are strongest when they are not associated with anything related to the user, and are not words found in a dictionary (even foreign dictionaries).

e. New passwords should not be the same password as chosen by the user for the last three (3) password cycles.

f. Passwords must not be written down or documented in any way. The display and printing of passwords must be masked or obscured. Passwords must not be stored in readable form in batch files or in log-in scripts.

g. All passwords must be promptly changed if they are suspected of being disclosed or are known to have been disclosed to unauthorized parties.

h. Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user; to do so exposes the authorized user to responsibility for actions that the other party takes with the password.

i. All vendor-supplied default passwords must be changed before any system is used.

j. A user will be locked out after three (3) invalid attempts to log in.

k. Computer screens will automatically lock if activity does not occur for 20 minutes to prevent unauthorized access and a password is required to unlock.

l. Staff must lock their computer when leaving the workstation. Manual workstation locking is accomplished by pressing the Windows Key and L simultaneously or pressing Ctrl Alt Delete and selecting Lock This Computer from the screen prompt.

m. Virus protection, perimeter defense/firewall technology, and anti-spyware intrusion detection software on computers are updated regularly and such software cannot be disabled by the user.

n. Regularly scheduled PC updates are installed requiring weekly reboot of all PCs.

o. All PCs are locked, and software cannot be installed without approval of an administrator.

p. Computer screen placement should reduce the chance that a passerby might see PHI.

5. **Fax*:*** Fax machines will be in secure locations and be monitored regularly for incoming documents. All unretrieved faxes containing PHI will be shredded at the close of each business day. Automatic pre-programmed fax dialing should be used on the fax machine (when possible) to help avoid incorrect dialing and a subsequent breach of PHI. All outgoing faxes must have a cover sheet with a confidentiality statement (see below for sample wording).

   Confidentiality Notice: This message, including any attachments, is for the sole use of the intended recipient(s) and may contain information that is confidential, privileged and/or exempt from disclosure under applicable law. Any unauthorized review, use, disclosure, or distribution is prohibited. If you are not the intended recipient, please contact the sender and destroy all copies of the original message

6. **Scan:** Documents scanned are saved automatically to the secured network. Once finished processing, the physical documents shall be shredded or stored according to the standards for Storage of PHI mentioned previously in this Section.

7. **Computer Network**: A virtual firewall that restricts all access into Agency's network except for approved VPN connections and Internet access controls are used to restrict certain users to access only approved web sites for business needs. Staff must not establish modem connections or other methods for networking which might enable unauthorized persons to gain access to PHI. Wireless LAN connections should only be used if WPA3 or higher levels of security and encryption are enabled.

8. **Workstation Inventory**: Maintain an inventory list/security log of the workstations that are considered staff workstations, listing the date, type of workstation computer, serial numbers, model

number, permitted user name(s) and server location(s). This will assist in tracking authorized users and assuring physical safeguards for these workstations.

9. **Encryption and E-Mail:** Software is used to encrypt and decrypt ePHI so that it is deemed unusable, unreadable, or indecipherable, provided there has not been a breach. For data "in motion," the encryption shall comply with the HHS Federal Information Processing Standard ("FIPS") Publication 140-2. For data "at rest," the encryption shall comply with the National Institute of Standards and Technology ("NIST") Special Publication 800-111.2. To ensure file integrity during data transmission is maintained, all data transmitted by electronic means whether by e-mail, physical media, or over a wide area network is encrypted. Content in subject lines is NOT encrypted and therefore, should not contain ePHI. It is prohibited to send ePHI over e-mail to the general public. The Agency has the right to monitor both internal and external e-mails (incoming and outgoing) to assure the security of PHI.
10. **Shredding**: Documents containing PHI, which are not safely filed, will be shredded onsite before disposal using the shredder or placing the documents in a locked shred bin. Staff will assure that shred bins are locked and also that the shred bins are not filled so high as to permit removal of unshredded PHI documents.
11. **Media Reuse & Disposal**: Media originally containing ePHI, which is planned to be replaced may only be redistributed to other State facilities provided the receiving facilities must agree not to sell or transfer said media outside the State department or agency and make no attempt to use techniques to recover ePHI formerly stored on media. Any ePHI stored on media to be replaced will be archived if required by existing retention policies and procedures. Staff will ensure all ePHI is systematically erased from the media before replacement or disposal. Prior to disposal, media containing ePHI must be rendered permanently inoperable consistent with National Institute of Standards and Technology ("NIST") Special Publication 800-88 so that ePHI cannot be retrieved by any known recovery method.
12. **Pictures Taken By Portable Devices**: Staff are not allowed to take pictures or video recordings of any documents or computer screens containing PHI with any portable device including but not limited to a camera or cell phone.
13. **Remote Access**: Staff must use an approved VPN connection to remotely connect to the agency network if agency's business plan allows remote work.
14. **Termination of Employees**: Upon final departure, terminated employees must surrender access key cards, ID cards, and any encoded tools used to gain access to ePHI. All network, computer, email, VPN, and any other access accounts for terminated employees must be disabled or deleted upon date of termination.

ADDITIONAL RESOURCES

45 CFR, Section 164.530(c)

Sample HIPAA Breach Log

Date of Breach	Date of Discovery	Description of Incident	Number of Individuals Affected	Notifications Made	Comments