All Affiliate Research Policy

Subject: HIPAA Security
For Researchers

File Under:
ORA HIPAA Security

Issuing Department:
Office of Research Administration

Original Policy Date
May 9, 2005

Page 1 of 5

Approved by:

Peggy McNeill, Director

Revision -

1) **Purpose:** Researchers will comply with the HIPAA Security Rule requirements as articulated in this policy and in the Lifespan corporate policies and procedures. Lifespan is committed to ensuring the security of electronic patient health information (EPHI) as required by 45 CFR Parts 160, 162 and 164.

2) **Scope:** This policy applies to Research Administration, all Researchers and their staff.

3) **Policy:**
   a) Lifespan HIPAA Security policies and procedures apply to the security of all EPHI and IT resources used to create, access, store and/or transmit EPHI. Lifespan has approved 18 policies and procedures that apply to HIPAA Security. These policies and procedures can be found on, or cross referenced on, http://intra.lifespan.org/compliance/security/documents
   b) Please refer to the policy for complete details and Lifespan's compliance guidelines. The table below summarizes Lifespan's corporate policies relating to the 18 HIPAA Security corporate standards.

#	Title	Policy Statement	SUMMARY
1	Security Management Process **Policy # HSP-80**	Security violations involving Electronic Protected Health Information (EPHI) should be prevented and, to the extent possible, detected, contained and corrected. Administrative, organizational, technical, and physical controls should be in place to support Lifespan's operational implementation of this policy.	• Identify systems that store EPHI • Assess risks • Apply sanctions for failure to comply • Review audit logs, if available, regularly • Review policies & procedures; make them available to workforce; maintain for 6 years

2	Assigned Security Responsibility **Policy # HSP-81**	The Lifespan Security Official is responsible for the development, implementation, maintenance and monitoring of policies, procedures, and information infrastructure required to maintain compliance with the HIPAA Security regulations.	• Identify security official to ensure accountability. • Mike Izzo is Corporate HIPAA Security Officer
3	Workforce Security **Policy # HSP-82**	Members of Lifespan's workforce should have appropriate access to EPHI based on their job descriptions, responsibilities and approval of the individual to whom they report. Access to EPHI should be restricted to the workforce members whose job description and responsibilities necessitate the use EPHI.	• EPHI restricted to specific workforce, define who • Workforce ID badges, access granted • EPHI restricted to job description
4	Information Access Management **Policy # HSP-83**	Access to EPHI should be controlled based on business and security requirements. Privileges granted should be based on "need-to-know", "minimum necessary" and/or "least privilege" criteria	• Monitor for only authorized access of EPHI • Grant access to PHI • Lists standards for granting access • Evaluate process
5	Security Awareness and Training **Policy # HSP-84**	A security awareness and training program for Lifespan workforce members and their contractors should be developed and supported on an on-going basis.	• All members of workforce required to have HIPAA Security training
6	Security Incident Readiness **Policy # HSP-85**	Lifespan members should be able to identify and respond to suspected or known information security incidents and attempt to mitigate, to the extent practicable, harmful effects of security incidents.	• Address unauthorized access, use, disclosure and/or destruction of an IS system • Document process and outcome
7	Contingency Plan **Policy # HSP-86**	A Contingency Plan or Plans should be developed, periodically tested, managed and maintained for all critical business functions and systems with the goal of maintaining availability, integrity, and confidentiality of EPHI during an emergency or other occurrence that damages systems that contain EPHI.	• Have a back up retrievable plan • Have a disaster recover plan
8	Evaluation **Policy # HSP-87**	In order to identify and address environmental or operational changes that could affect the security of Electronic Protected Health Information (EPHI), Lifespan should periodically conduct a technical and non-technical evaluation to assess compliance of security policies and procedures against HIPAA Security Standards.	• Periodically evaluate compliance

9	Use of Business Associate Agreements (BAAS) **Policy # HSP-CCPM-56**	Lifespan department managers and directors are responsible for identifying BA relationships (see CCPM-56A for help). They should notify Lifespan IS or Corporate Compliance when a new BA is identified so that one of these departments can initiate and document the BAA contracting process. Lifespan has a model BAA that contains all provisions mandated by HIPAA privacy and security. This model should always be used when contracting with a BA, unless specific permission to do otherwise is granted by IS, Corporate Compliance or the Office of the General Counsel.	• BAA revised to include all provisions mandated by HIPAA privacy and security • Need to identify BAs • Notify IS or Corporate Compliance of new BA
10	Facility Access Controls **Policy # HSP-89**	Lifespan's Information Technology (IT) equipment, information processing facilities, user computers and records should be physically protected from security threats and environmental hazards. Security safeguards and controls should be in place to prevent unauthorized access to electronic information, loss or damage to physical assets or interruption to business activities.	• Limit physical access to facility and equipment • Contingency facility access plan
11	Workstation Use **Policy # HSP-90**	Workstations should be configured and maintained with appropriate security controls to protect confidentiality, integrity, and availability of EPHI. Security safeguards and controls should be implemented to protect unattended workstations from unauthorized access and to secure the physical surroundings of the workstations.	• Prevent unauthorized use and disclosure of EPHI from workstations. • Firewall protection • Theft deterrent device or tracking software for public computers • Utilize security controls-logon, etc
12	Workstation Security **Policy # HSP-91**	Security safeguards and controls should be implemented for the physical protection of workstations that access EPHI so that confidentiality, integrity, and availability of EPHI are not compromised.	• Physical safeguards • Laptops – screen guards, secure from theft, secure in locked cabinets • PDA encrypt, password protect
13	Device & Media Controls **Policy # HSP-92**	Security safeguards and controls should be adopted for protecting EPHI in the event of re-use, transfer, storage or disposal of electronic media or devices.	• Storage, disposal, re-use, accountability, data back-up & storage of equipment with EPHI • Delete files, reformat

14	Access Controls **Policy # HSP-93**	Access to electronic information systems that maintain EPHI should be restricted and controlled. Access to EPHI should be granted on a minimum necessary basis that reflects the minimum amount of information necessary for an authorized person to complete the tasks and responsibilities of his or her job function. Security safeguards and controls should be in place to protect against unauthorized access attempts.	• Unique user ID • Encrypt, decrypt, auto logo • IS specific policy • Encrypt laptops and PDAs
15	Audit Controls **Policy # HSP-94**	Access and changes to EPHI in certain designated information systems should be periodically monitored and logged. Where appropriate, activity logs should be maintained.	• If feasible log user activity • If not feasible document why no audit trail (software does not have ability to audit trail, etc.)
16	Integrity **Policy # HSP-95**	Security safeguards and controls should be established to protect EPHI from unauthorized alteration or destruction.	• Technical controls – no unauthorized software on computers
17	Person/Entity Authentication **Policy # HSP-96**	Access to Electronic Protected Health Information (EPHI) should be provided to a person or an entity only after verifying that the person or entity seeking the access is the one claimed and that the person or entity has been authorized to receive access.	• Verify authorized user
18	Transmission Security (email) **Policy # HSP-97**	Confidentiality, availability, and integrity of EPHI should be maintained by implementing security safeguards and controls when transmitting information between authenticated parties over electronic communications networks.	• Email – use only Lifespan email, will be encrypted • Log on to secure sites only • Brown email addresses should not be used to transmit EPHI

4) Procedure:

a. Researchers will, whenever possible, follow the above 18 HIPAA Security policies and procedures adopted by Lifespan.

- The corporate policies and procedures will apply to all Lifespan employees, all researchers and their staff, and all equipment and software issued and maintained by Lifespan and its affiliates. When using Lifespan computers and software or any other computer or software it is recommended researchers double protect the EPHI documents by password protecting the documents.

b. When researchers use non-Lifespan equipment and/or software, not issued or maintained by the Lifespan IS department, it is recommended that the software and/or equipment be HIPAA Security compliant. The recommendations and requirements listed in the 18 policies and procedures referenced above should be applied, whenever possible, to this equipment and/or software.

a. Password protection to all computers and equipment should be instituted.
b. Password protect all documents whenever possible.
c. PDA and laptops – Password protect equipment and double protect by password protecting documents on equipment
d. Encryption software, whenever possible, should be installed on equipment and used for storing/transmitting EPHI.
e. Take security precautions for theft or loss of equipment, locked cabinets, etc.

c. When researchers log on to a sponsor or multi-site website, or any other website used for the purposes of this research protocol, to upload EPHI it is recommended this EPHI be uploaded to secure websites. If websites are not secure it is recommended researchers use alternate methods of transmission of EPHI such as: de-identify data if possible, paper fax whenever possible, copy to CD and carry or secure mail to recipient.

d. Audit trails should be turned on and monitored. When audit trails are not possible because the software does not support audit trails this should be documented. Examples would be – Excel spreadsheets, Access spreadsheets, etc.

e. Email, file transfer and encryption – It is recommended researchers use Lifespan email when sending EPHI as an attachment. The attachment should have an additional level of protection by password protecting the document.

a. Use of other email for sending attachments containing EPHI is not recommended. However, if use of non-Lifespan email for attachments is employed encrypt document.
b. De-Identify document whenever possible prior to email
c. Copy to CD and carry or secure mail to recipient
d. Paper fax document if unable to de-identify data or use secure method

f. Only authorized personnel, researcher/staff/sponsor, etc., should have access to Research data. Reports of unauthorized user access, disclosure or destruction should be reported to the ORA.

g. Researchers should back up their research data, i.e., CD/floppy, if not stored on Lifespan computer share drive or Sponsor site.

h. Researchers will certify on an annual basis to comply with recommendations and requirements, whenever feasible, as listed on the ORA HIPAA Security Certification Form.

i. The HIPAA Security Investigator Certification form will be provided to all investigators annually on or near re-certification date when new or continuing applications are submitted to the Office of Research Administration Research Review Committee and Communications for review.

j. This HIPAA Security Policy will be provided to all investigators with the annual Certification form. Investigators are encouraged to review this policy and the 18 HIPAA Security policies prior to certifying compliance.

k. Annual HIPAA Privacy and Security training for researchers is required of Research Administration and all researchers and their staff. HIPAA training certification will continue to be addressed on IRB submission forms.