

	Johns Hopkins [insert provider or plan name]	Policy Number	C.2
		Effective Date	04/20/05
	PROVIDERS and HEALTH PLANS	Page	1
	ADMINISTRATIVE SECURITY POLICIES	Supercedes	

HIPAA Security Regulations require covered entities to protect the security of patient and plan member information. Information security related to HIPAA is addressed in four policies:

1. *General Policy on Security Regulations* (HIPAA Policy C.1)
2. *Administrative Security Policies* (HIPAA Policy C.2)
3. *Physical Security Policies* (HIPAA Policy C.3)
4. *Technical Security Policies* (HIPAA Policy C.4)

In addition to the above security policies, protection of E-PHI also is subject to all applicable privacy, information technology and other policies.

DEFINITIONS

E-PHI means PHI which is (1) transmitted by electronic media or (2) maintained in electronic media.

E-PHI System means a system owned by and/or administered within Johns Hopkins and all applications and data contained on such system that process, store or transmit E-PHI, and principally include servers, database applications, networks, e-mail systems and Web applications. Workstations, other devices and supporting software (e.g. operating systems, Web servers, etc.) used to access E-PHI are considered components of E-PHI Systems. A workstation or other device that stores substantial amounts of E-PHI in any form – including as a spreadsheet, word processing document, or e-mail client – generally is deemed to be an E-PHI System and subject to all Johns Hopkins HIPAA Security Policies.

HIPAA means the Health Insurance Portability and Accountability Act of 1996.

Johns Hopkins means the Johns Hopkins covered entity that adopted this policy.

PHI means protected health information, i.e., individually identifiable health information.

Responsible Administrator means the senior manager for a Responsible Site who has responsibility for overseeing E-PHI and E-PHI Systems and for assuring compliance with HIPAA security policies and HIPAA privacy policies for such Site (working with other Responsible Administrators where appropriate).

Responsible Site means those entities or functional areas that have been charged with the administrative oversight responsibilities for compliance with the Privacy and Security Regulations. [Click here](#) for a listing of Responsible Sites.

Security Regulations means the regulations promulgated by the Secretary of the Department of Health and Human Services to implement portions of HIPAA that concerns the security of electronically transmitted or maintained health information, as amended from time to time; these regulations currently include 45 CFR §§ 160 and 164, subparts A and C.

Vendor means a vendor, consultant, contractor or other non-Johns Hopkins third party who may have access to E-PHI or an E-PHI System for any reason or purpose (other than those who may have

incidental access) or the Johns Hopkins facilities housing the information technology assets that support E-PHI or E-PHI Systems or related infrastructure.

Workforce members, for purposes of this policy only, are persons under the direct or indirect control of Johns Hopkins, including, but not limited to, employees, students, interns, residents, fellows, researchers, staff, faculty, volunteers and temporary personnel.

A. POLICY – RISK ASSESSMENT

Every E-PHI System, and all administrative, physical and technical issues associated with E-PHI Systems, shall be assessed periodically for security risks.

REQUIREMENTS

The Security Regulations require that security compliance meet a reasonableness standard. Determining what is reasonable for a specific system or entity requires on-going risk assessment. Responsible Sites must undertake and document risk assessment for all E-PHI Systems, addressing, without limitation, the following:

1. system purpose
2. threats
3. vulnerabilities
4. risk
5. controls
6. damage mitigation
7. cost effectiveness of controls
8. metrics for evaluation of effectiveness.

Risk assessment is principally concerned with two variables: (1) likelihood of security compromise and (2) damage from such a compromise. Security controls are implemented to remediate vulnerabilities in systems in order to meet threats effectively.

Every instance of E-PHI and each E-PHI System present different types and levels of risk. When prioritizing a security strategy and controls, Responsible Sites must consider, without limitation, the following risk factors:

1. amount of E-PHI
2. relative sensitivity of E-PHI (e.g. psychiatric records have a high sensitivity)
3. number of authorized users
4. number of concurrent users for an application
5. architecture (e.g. Internet access, remote users).

Systems that rate a high risk according to these factors should be identified as such by Responsible Sites. Such high risk E-PHI Systems are to be addressed on a priority basis and given the most stringent security controls practical.

[References: HIPAA Regs.--Section 164.308(a)(1)(ii)(A)]

B. POLICY – RISK MANAGEMENT

Standards for handling E-PHI and maintenance of E-PHI Systems are mandatory for all Responsible Sites. If implementation of a required control is impracticable, variance(s) from Johns Hopkins policies, requirements and standards shall be documented and appropriate compensating control(s) shall be implemented.

REQUIREMENTS

Security controls that suffice in one environment, for example billing, may be inappropriate in clinical or research settings. Effective security requires a series of trade-offs. In some cases confidentiality may conflict with equally important considerations of data availability or system usability. For a number of E-PHI Systems, it will be impractical, for reasons of technology or practice, to implement every requirement. It is the responsibility of each Responsible Site therefore to:

1. identify variances from Johns Hopkins policies, requirements and standards
2. state reasons for such variances
3. address risks posed
4. identify planned or implemented compensating controls.

In many cases, such variances are dictated by limitations in technology, and policy and/or practice can be used to achieve the objective of the security requirement.

[References: HIPAA Regs.--Section 164.308(a)(1)(ii)(B)]

C. POLICY – ACCESS TO E-PHI -- AUTHORIZATION

Johns Hopkins shall ensure that only those workforce members and vendors who have a business need to access E-PHI and/or E-PHI Systems are authorized to have access to such E-PHI and/or E-PHI Systems.

REQUIREMENTS

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document a process to determine whether each of its workforce members and each of its vendors has a need for access to E-PHI or to E-PHI Systems in order to perform his/her job functions or to provide contracted services. Such a process shall, without limitation, include:

1. evaluate access to E-PHI based on a workforce member's or vendor's need to know for appropriate business purposes,
2. conduct background checks when appropriate (for example, workforce members with system administrative rights),
3. provide to each workforce member a written statement of access rights to E-PHI Systems and an acknowledgement of those rights and responsibilities to be signed by the workforce member or vendor.
4. maintain a formal process for documenting and reviewing complete lists of workforce members and vendors authorized to access E-PHI ,
5. communicate with human resources departments and other systems owners to revise or terminate access rights in a timely manner,
6. designate an individual to manage authorization procedures – including account creation, modification, termination and emergency access, and

7. assess effectiveness of access controls on a regular basis incorporating access and activity logs and incident reports.

[References: HIPAA Regs.--Section 164.308(a)(3) and (4)]

D. POLICY—WORKFORCE TRAINING—SECURITY

Johns Hopkins shall provide appropriate training on the Security Regulations and Johns Hopkins' security policies to all workforce members who have access to E-PHI.

REQUIREMENTS

1. Department management shall train or see to the training of all workforce members who have access to E-PHI on security policies and procedures as necessary and appropriate for workforce members to carry out their job functions.
2. Department management is responsible for ensuring that new workforce members who have access to E-PHI complete the appropriate security issues course(s) on the on-line HIPAA training system, and receive any other appropriate security training before gaining access to E-PHI in order to perform their job function,
3. Evidence of each workforce member's successful completion of HIPAA training should be retained by the workforce member's department management and in the workforce member's human resource general personnel file, at a minimum.
4. Each Responsible Site is responsible for ensuring that its workforce members have received appropriate training whenever the workforce member is acting in a role of a systems or security administrator.
5. If any Johns Hopkins security policies or requirements are substantially changed, all affected workforce members shall be trained in the new policy or requirement within two (2) months of the policy's or requirement's effective date. Johns Hopkins will use existing mechanisms to inform workforce members of these changes and will provide more detailed training, where deemed necessary.

[References: HIPAA Regs.--Section 164.308(a)(5)]

E. POLICY—SECURITY INCIDENT PROCEDURES

Responsible Sites shall address attempted and successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations with respect to their E-PHI Systems.

REQUIREMENTS

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document and implement procedures to report immediately significant security incidents to appropriate Johns Hopkins personnel and coordinate responses accordingly.

1. *Technical Reporting* -- Workforce members should report incidents such as virus attacks or other device anomalies to appropriate technical staff (e.g. server or workstation support, application support, help desk, department manager). It is the responsibility of technically knowledgeable staff to evaluate user reports and report information security incidents to the Johns Hopkins

Computer Incident Response Team (CIRT), with particular attention to incidents that have the potential to damage network operations.

2. *Physical Security Reporting* -- incidents that principally involve theft, defacement or other illegal activity should first be reported to the respective campus or health system physical security department. Physical security departments shall coordinate with the Johns Hopkins Chief Information Security Officer to investigate and evaluate potential compromises of E-PHI.
3. *Documentation* -- Responsible Sites shall log and monitor reports of security incidents including response actions and outcomes.

If the nature of the incident concerns principally unauthorized access to PHI, in electronic or other form, it should first be reported to the Johns Hopkins Privacy Officer for handling in the nature of a privacy complaint. The Johns Hopkins Privacy Officer will work with the Johns Hopkins Chief Information Systems Officer to evaluate the information security implications of such incidents and process the report accordingly.

[References: HIPAA Regs.--Section 164.308(a)(6)]

F. POLICY—CONTINGENCY PLANS

Responsible Sites shall document disaster recovery and business continuity planning. Business critical E-PHI Systems shall have comprehensive disaster recovery and business continuity plans.

REQUIREMENTS

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document, disaster recovery and business continuity planning consistent with institution-wide plans, policies and procedures for E-PHI Systems. For business critical systems, meaning those systems for which failure or down-time would significantly impact a business mission of all or part of Johns Hopkins or otherwise pose a risk of loss or disclosure of E-PHI, disaster recovery and business continuity plans must be implemented and tested. All E-PHI Systems must document the following:

1. Analyses of data criticality -- considers importance to business mission and data sensitivity
2. Data back-up processes -- in accordance with requirements set forth in Section C of Physical Security Policies (HIPAA Policy C.3)
3. Recovery procedures -- procedures to restore any loss of operational capacity or data

Business critical E-PHI Systems must also include the following:

4. Emergency operating procedures -- detailed procedures for maintaining critical business operations and for the protection of E-PHI while operating in an emergency mode
5. Testing and revision processes -- regular testing, coordinated with institutional tests and documented. Emergency plans must be revised as appropriate, stored on-site near critical systems and available off-site at an accessible location.

[References: HIPAA Regs.--Section 164.308(a)(7)]

G. POLICY - EVALUATION

All E-PHI Systems are required to undergo evaluations at least once every two (2) years. Security evaluations are performed by Responsible Sites to evaluate risks, identify and test security controls, and update risk management plans.

REQUIREMENTS

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document, and implement, a process to evaluate each E-PHI System that includes::

1. description of purpose and inter-dependent systems
2. detailed statement of system owners, administrators and departmental links
3. integration architectures and access methodologies (including remote access) and diagrams
4. statement of security strategy and any compliance or policy changes
5. changes in threat and risk environment
6. update of implemented controls
7. account of data security incidents
8. discussion of disaster recovery plan and procedures
9. training update for users and administrators
10. implementation plan for new or updated physical, administrative and technical controls.

[References: HIPAA Regs.--Section 164.308(a)(8)]

H. POLICY -- RECORD, RETENTION AND DESTRUCTION

All plans, reports, evaluations and other documentation of risk management and compliance strategy shall be retained in conformity with the HIPAA Privacy Policy A.8.9-Retention and Destruction.