

	Johns Hopkins [insert provider or plan name]	Policy Number	C.4
	PROVIDERS and HEALTH PLANS	Effective Date	04/20/05
		Page	1
		TECHNICAL 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 – ACCESS CONTROL/AUTHENTICATION

Access to E-PHI and to E-PHI Systems shall be allowed only to those workforce members, vendors or software programs that have been granted access rights pursuant to Administrative Security Policy (HIPAA Policy C.2, Section C). Unique user identification and effective user and entity authentication are required for E-PHI Systems.

REQUIREMENTS

1. Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures that include the following access controls:
 - a. Access control procedures (including authorization, administrator access, authentication, termination and emergency access)
 - b. Issuance of unique (not shared between multiple users) user ID's with appropriate authentication mechanisms (e.g. passwords, tokens, etc.)
 - c. Efforts to move from single factor to multi-factor authentication (e.g. biometric, tokens) and to use single sign-on (SSO) for E-PHI Systems
 - d. Emergency access procedures for users and administrators and responsible individuals designated
 - e. Procedures for automatic log-off of users after a predetermined time of inactivity.
2. Unique user IDs combined with passwords are now the most common form of authentication for Johns Hopkins applications/systems, and it is critical that E-PHI Systems demonstrate rigorous password management. For access to E-PHI Systems authentication technologies and practices must incorporate the following:
 - a. Creation or issuance of hard-to-guess (strong) passwords that contain a combination of letters, numbers and special characters and are at least eight (8) characters in length
 - b. Lock user accounts after five to ten (5 - 10) unsuccessful login attempts
 - c. Forced periodic password changes (i.e. a period of 90 to 180 days is typical)
 - d. Prohibition of password re-use
 - e. Prohibition of disclosure of passwords intentionally (e.g. disclosed over the telephone) or unintentionally (e.g. written down near the access point or maintained in an accessible electronic file, displayed during key entry). For occasional maintenance or trouble-shooting, it may be necessary for a user to disclose a password to a system administrator. In such cases, it is the user's responsibility to change passwords as soon as practical
 - f. Users are to access E-PHI Systems only through their own access authorization and not through another user's account.

[References: HIPAA Regs.--Section 164.312(a)(1) and (2) and (d)]

B. POLICY – ACCESS CONTROL/REMOTE ACCESS

Access to E-PHI Systems from external locations (i.e., remote access) is granted only to approved devices and pathways and only for specific users and purposes. The same level of protection shall be maintained for E-PHI that is stored or accessed remotely as for information stored or accessed in the Johns Hopkins network. E-PHI Systems must have effective authentication of remote users and devices as well as strict monitoring of remote access.

REQUIREMENTS

1. Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures in the following categories for securing remote access to E-PHI Systems:

a. *Authentication/Identification* – strong authentication, preferably a form of multi-factor authentication

b. *Malicious software* – reasonable technical and/or policy efforts to ensure that remote devices are updated and patched as appropriate

c. *Data Interception* – remote access to high risk E-PHI Systems must be protected by appropriate encryption technologies such as Secure Sockets Layer (SSL) and/or Virtual Private Networks (VPN).

[References: HIPAA Regs.--Section 164.312(a)(1) and (2) and (d)]

C. POLICY—AUDIT CONTROLS

Johns Hopkins shall implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use E-PHI. E-PHI Systems must log access, and where feasible, activity. Audit processes must be implemented to examine logged information.

REQUIREMENTS

1. Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures for auditing access to and use of E-PHI Systems in order to:

a. identify questionable data access activities

b. investigate breaches

c. respond to potential weaknesses (in coding and systems architecture(s))

d. assess the effectiveness of a security program.

2. All E-PHI Systems are required to include audit capabilities for the following purposes:

a. *Access logs* – Auditing is required to monitor unauthorized access

b. *Audit planning* -- Each Responsible Site is required to assess and document the most cost-effective manner for producing audit logs for each E-PHI System. Audit logging should be deployed in layers: at the network, application and back-end database level

c. *Monitoring* – Audit logs must be reviewed at intervals appropriate to applicable levels of risk.

3. In addition to the requirements above, all high risk E-PHI Systems are required to include the following robust audit capabilities:

a. *Access logs* - E-PHI Systems at Johns Hopkins must log each user's access to the system from log-on to log-off.

b. *Activity logs* -- High risk E-PHI Systems must maintain activity logs linking users to actions on the system. While it is recommended that activity logs have the capability to record changes made by the user, it is required only that these logs provide the basis for helping to determine whether changes were made by a specific individual to a patient or plan member record.

[References: HIPAA Regs.--Section 164.312(b)]

D. POLICY – INTEGRITY

Johns Hopkins shall implement procedures to protect E-PHI from improper alteration or destruction. E-PHI must be protected through sound security practices regarding the underlying information infrastructure.

REQUIREMENTS-- PROTECTION OF SYSTEMS

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures for securing E-PHI by a robust and pliable network architecture and well-protected servers, workstations and devices that incorporate at least the following:

1. *Disabling Unnecessary Services* – E-PHI Systems must disable those services that are not required to achieve the business purpose of the system (e.g. FTP, Telnet, SMTP, etc).
2. *Virus Protection* – E-PHI Systems and all related machines must maintain automated virus update mechanisms. Updates should be automatic and transparent where practical, otherwise automatic reminders are required. It also is recommended that controls be implemented to protect against other malicious software as threats evolve (e.g. spyware).
3. *Patch Management* – E-PHI Systems must have controls in place to provide timely notification regarding relevant patches. Responsible Sites have the responsibility to determine whether and/or when to deploy patches. In cases where IT@JH recommends deployment of a patch, Responsible Sites must deploy patches in a timely fashion or otherwise implement documented compensating controls.
4. *Intrusion Detection* – networks that support processing, storage, or transmission of E-PHI must be monitored for intrusion and compromise by current and effective intrusion detection and/or prevention technologies. Intrusions must be audited, logged and, where appropriate, reported through the Johns Hopkins incident reporting process (Administrative Security Policies (HIPAA Policy C.2, Section E). Where intrusions have resulted in or are likely to result in compromises of E-PHI they must be reported through the Johns Hopkins incident reporting process. Host-based or application level intrusion detection is also a recommended best practice.
5. *Server Security* – server administration functions may be performed only by authorized and trained personnel. Remote administration of E-PHI Systems requires strong authentication, stringent authorization, encryption, and regular review of complete administrator access logs.
6. *Workstation Security* – workstation administration functions must be performed only by authorized and trained personnel. Any workstation with access to E-PHI requires unique individual log-in passwords and a mechanism for suspending user access after a period of inactivity (e.g. requiring re-authentication after twenty (20) minutes). For workstations that do not require unique individual passwords, suspension of access to E-PHI must occur at the application level. No E-PHI may be stored on workstations that do not require unique individual passwords.
7. *Mobile Devices* -- no E-PHI may be stored on mobile devices (e.g. laptops, PDA, tablet PC's, etc.) unless the device uses (a) unique individual power-on passwords, (b) password-protected screen savers, *and* (c) all stored E-PHI is protected in password protected files. It is recommended that such files be encrypted.
8. *Vulnerability Scanning* -- regular monitoring of equipment for vulnerabilities, specifically regarding components connected to Johns Hopkins networks. Responsible Sites shall cooperate with Johns Hopkins network security teams on network scanning and vulnerability remediation.

[References: HIPAA Regs. --Section 164.312(c)]

REQUIREMENTS-- DATA SECURITY/INTEGRITY

1. Subject to the General Policy on Security Regulations (HIPAA Policy C.1), Responsible Sites must document a process to assess regularly data storage and processing requirements in order to reduce risk of compromise of data confidentiality and/or integrity. Protection of stored E-PHI must utilize layered controls at network, application and database levels.
2. Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures to secure confidentiality and protect data from improper alteration or destruction by implementing controls appropriate to the level of risk as stated in Administrative Security Policies (HIPAA Policy C.2, Section A).⁴¹ The following includes several best practice controls:
 - a. All E-PHI is to be secured at the application and underlying database levels. Substantial amounts of E-PHI must be stored in a manner that supports user access logs and strong authentication of users and administrators.

b. E-PHI at rest must be protected appropriate to inherent risk. Small aggregations of E-PHI, including spreadsheets, must be password-protected (see Section A above). Greater risk would necessitate more stringent controls, including stronger password management, access logs and close monitoring.

c. Back-end databases, specifically those with substantial amounts of E-PHI, must be actively protected. Back-end databases containing E-PHI must be isolated from other application or system services (e.g. application middleware, Web and e-mail servers, etc.), and where not practical, compensating controls must be implemented.

[References: HIPAA Regs.--Section 164.312(c)]

E. POLICY—TRANSMISSION SECURITY

Johns Hopkins shall implement measures to guard against unauthorized access to E-PHI that is being transmitted over an electronic communications network. A mix of appropriate technologies and practices must secure all transmissions of E-PHI. Transmissions of E-PHI across public networks, such as the Internet, must be secured through appropriate controls and feasible controls.

REQUIREMENTS

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures to secure data during transmission (including, without limitation, e-mail and file transfers). Any transmission of substantial amounts of E-PHI over the Internet must be encrypted. It is the responsibility of Responsible Sites and all workforce members to protect all transmissions of E-PHI appropriate to the level of risk.

1. Responsible Sites must address the following technical security safeguards when transmitting E-PHI over public networks, such as the Internet:

- a. *Integrity controls* – ensure that data have not been tampered with by unauthorized users
- b. *Sender authentication* – ensure that the sender is who she purports to be
- c. *Access controls* – ensure that data access is strictly limited
- d. *Recipient authentication* – ensures that data reach intended recipient(s) and only intended recipient(s)
- e. *Encryption* – standards-based encryption protects data confidentiality in transit
- f. *Event reporting* – system failures or compromises are flagged and reported in a timely fashion
- g. *Audit* – records allow for trace of user actions appropriate to the level of risk.

2. Many of the above controls are addressed by the appropriate use of security technologies (e.g. IPsec-compliant virtual private networks (VPNs), TLS over SSL, etc.) and practices. Additional standards for the use of e-mail in communicating E-PHI are provided below:

a. E-mail is inherently insecure, and most common uses of e-mail are vulnerable to attack. Senders must address the following:

- (i) The possibility of sending e-mail to an incorrect e-mail address, therefore senders should verify e-mail addresses
- (ii) Because some e-mail addresses are shared, even a correctly addressed message may not be private, and senders should verify intended recipient(s)
- (iii) To protect the confidentiality of E-PHI in e-mails, senders must use encrypted e-mail services where such services are available and practical.

b. The inclusion of E-PHI in e-mail must be limited to the *minimum necessary* information to meet the intended purpose(s) and directed only at personnel with a legitimate *need-to-know*.

c. Instant messaging and similar technologies (e.g. alpha text paging) has many of the same security defects as e-mail, and is generally even more difficult to secure. Unless the communicating parties are certain that communications are protected effectively against unauthorized use or disclosure (e.g. provided by encryption on public networks, use of dedicated networks, etc.), E-PHI may not be sent through instant messaging.

[References: HIPAA Regs.--Section 164.312(e)]

F. 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.

^[1] For example, controls appropriate for a spreadsheet with E-PHI on a handful of patients or plan members should be substantially different from those on high-risk E-PHI Systems that have many authorized users and a substantial amount of E-PHI. It is the responsibility of Responsible Sites to evaluate and document the level of risk of each E-PHI System and to make appropriate decisions regarding controls.