

ARTICLE 3 SMALL GROUP HEALTH PLAN HIPAA SECURITY COMPLIANCE

THE REMEDIATION PROCESS: TECHNICAL VERSUS POLICY

Though much of Security has to do with computer systems, gaining user access and figuring out if you can still use email, many of the HIPAA Safeguard requirements revolve around administrative topics. Your organization will find itself establishing guidelines for items such as: access control, developing additional sanctions, making the workforce accountable for keeping their passwords confidential, and getting updated Business Associate Contracts.

For most Group Health Plans, realizing that HIPAA Security is both a technical and a policy project means some major things.

- 1. Senior Management is going to have to:**
 - a. Understand**
 - b. Provide the budget**
 - c. Provide the resources**
 - d. Support cross-functional meetings with a global team not unlike the one who dealt with Privacy (including the Privacy Officer, legal/regulatory/compliance experts, facilities management, operations representatives and of course plenty of system support).**
- 2. HIPAA Security cannot be addressed and “fixed” by IT. It will take significant communication with the Privacy Officer, other operational departments and the Third Party Administrator, if applicable. A constant open line of communication to deal with the huge task of performing an initial risk assessment and choosing the magical combination of technical solution and policy in order to address Security requirements will be needed.**

The ultimate goal of your HIPAA compliance is to “prove” your efforts by documenting that your workforce complies with your unique policies and procedures. Getting to the point where the policies and procedures are routinely followed by the workforce will be an ongoing process that requires constant monitoring.

Keeping you informed. Just one more reason to choose GBS.

HINT: If you have subcontracted much of your operations to a Third Party Administrator, you still need to consider YOUR direct workforce members *and* the TPA should be providing you proof that they have implemented policies and procedures that adhere to HIPAA on your behalf!

Our next feature will provide information about some of the more controversial topics you will need to explore while conducting your remediation efforts.

Group Benefit Services, Inc. has once again employed a HIPAA Consultant to help us through our Risk Analysis as well as assisting us in the preparation for internal training, completing our Policies and Procedures and developing documentation for our clients. GBS has been working with Lesley Berkeyheiser, of The Clayton Group, since last spring on HIPAA Security and how the regulations affect a TPA. We are pleased to be able to offer her consulting services to you as well.

Keeping you informed. Just one more reason to choose GBS.

6 North Park Drive, Suite 310 • Hunt Valley, MD 21030
410.832.1300 • 800.638.6085

www.gbsio.net

HIPAA SECURITY STANDARDS CHECKLIST

HIPAA requires covered entities to meet strict security standards for both electronic data and data maintained in more conventional formats such as paper. HIPAA's security standards are contained in two separate provisions: the Security Rules and the Privacy Rules. The Security Rules are effective April 20, 2005 (April 20, 2006 for a "small" health plan). The Privacy Rules are effective April 14, 2003 (April 14, 2004 for a "small" health plan).

The Security Rules have four main areas:

- Administrative Safeguards (such as policies and procedures and establishing a security official);
- Physical Safeguards (such as limiting access to computers to authorized individuals and making backup copies of electronic data);
- Technical Safeguards (such as establishing passwords on computers and encrypting or otherwise ensuring the integrity of emails); and
- Organizational Safeguards (such as ensuring that a business associate or, in some cases, a plan sponsor of a group health plan has adequate security provisions).

The Privacy Rules are similar and require:

- Administrative Safeguards (such as establishing policies and procedures stating how protected health information will be used or disclosed and who may access the information);
- Physical Safeguards (such as shredding paper documents, moving facsimile machines to a secure area and locking filing cabinets);
- Technical Safeguards (such as computers on passwords).

Although not contained as part of the Privacy Rules' safeguard provisions,¹ a covered entity also must require that its business associates implement similar safeguards of protected health information.²

MB&F Note: These standards are likely to apply "common sense" measures and are likely to be "scalable"—so, the larger the covered entity, the more that is required.³ Note that there is overlap between the requirements of the Security Rules and the Privacy Rules. Electronic protected health information generally will be subject to both standards.⁴ This can create some timing difficulties. For example, it likely requires a covered entity to adopt certain security

¹ These security standards are located at 45 C.F.R. §164.530(c).

² 45 C.F.R. §164.504(e)(2)(ii)(B).

³ 65 Fed. Reg. 82461, 82562 (Dec. 28, 2000).

⁴ 65 Fed. Reg. 82461, 82562 (Dec. 28, 2000).

standards for electronic protected health information by the effective date of the Privacy Rules—even though the standards are not required until 2005 (or 2006) under the Security Rules.

The following pages provide a detailed description of these requirements. The first section (and Appendix A) focuses on the Security Rules. The last section focuses on the Privacy Rules. Note that under the Security Rules each set of safeguards describes certain security standards (e.g., “Standard: Security Incident Procedures”). Under each security standard, a covered entity must meet certain implementation specifications. In some cases, the implementation specifications are “Required” and in other cases they are “Addressable.”

If an implementation specification is Required, a covered entity must comply with the specification. If an implementation specification is Addressable, the covered entity must 1) assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information, and 2) implement the specification if reasonable and appropriate or if implementing the specification is not reasonable and appropriate, document why it would not be reasonable and appropriate to implement and implement an equivalent alternative measure if reasonable and appropriate.

SECURITY SAFEGUARDS: ELECTRONIC PROTECTED HEALTH INFORMATION

ADMINISTRATIVE STANDARDS (45 C.F.R. § 164.308(a))

Administrative Safeguards.

- Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.
- Implementation specifications:**
 - Risk analysis (*Required*). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
 - Risk management (*Required*). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
 - Sanction policy (*Required*). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

MB&F Note: Plan sponsors may be required to update their employee handbook to ensure that these sanctions can be applied against workforce members who violate the security policies and procedures.

- Information system activity review (*Required*). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- Standard: Assigned security responsibility.** Identify the security official responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

MB&F Note: Like a “privacy official” under the Privacy Rules, a “security official” must be appointed for a self-funded group health plan that has electronic protected health information.

- Standard: Workforce security.** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (i.e., that they have the proper level of access), and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.

Implementation specifications:

- Authorization and/or supervision (*Addressable*). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
- Workforce clearance procedure (*Addressable*). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
- Termination procedures (*Addressable*). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made under the workforce clearance procedure, above.

- Standard: Information access management.** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with safeguards required under HIPAA.

Implementation specifications:

- Isolating health care clearinghouse functions (*Required*). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

MB&F Note: This requirement only applies to health care clearinghouses, a particular kind of covered entity. This requirement should not affect most group health plans.

- Access authorization (*Addressable*). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
- Access establishment and modification (*Addressable*). 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.
- Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).

MB&F Note: The term “workforce” can be confusing. The requirement only applies to the “workforce” of the covered entity (i.e., the group health plan) not the entire workforce of the plan sponsor.

- Implementation specifications.**
 - Security reminders (*Addressable*). Periodic security updates.
 - Protection from malicious software (*Addressable*). Procedures for guarding against, detecting, and reporting malicious software.
 - Log-in monitoring (*Addressable*). Procedures for monitoring log-in attempts and reporting discrepancies.
 - Password management (*Addressable*). Procedures for creating, changing, and safeguarding passwords.
- Standard: Security incident procedures.** Implement policies and procedures to address security incidents.
 - Implementation specification:** Response and reporting (*Required*). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
- Standard: Contingency plan.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Implementation specifications:

- Data backup plan (*Required*). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
 - Disaster recovery plan (*Required*). Establish (and implement as needed) procedures to restore any lost data.
 - Emergency mode operation plan (*Required*). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
 - Testing and revision procedures (*Addressable*). Implement procedures for periodic testing and revision of contingency plans.
 - Applications and data criticality analysis (*Addressable*). Assess the relative criticality of specific applications and data in support of other contingency plan components.
- Standard: Evaluation.** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS
(45 C.F.R. § 164.308(b))

- Standard: Business associate contracts and other arrangements.** A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.
- This standard does not apply with respect to (i) the transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual; (ii) the transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor (to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met); or (iii) the transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

- A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and these requirements.
- Implementation specifications:** Written contract or other arrangement (*Required*). Document the satisfactory assurances described above through a written contract or other arrangement with the business associate that meets the applicable requirements of HIPAA.

MB&F Note: If your contract with a service provider expires in 2004 (2005 for a small health plan) consider updating the contract at that time to incorporate the Security Rule provisions.

PHYSICAL SAFEGUARDS (45 C.F.R. § 164.310)

- Standard: Facility access controls.** Implement policies and procedures to limit physical access to the covered entity's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Implementation specifications:**
 - Contingency operations (*Addressable*). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
 - Facility security plan (*Addressable*). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
 - Access control and validation procedures (*Addressable*). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
 - Maintenance records (*Addressable*). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
- Standard: Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

- Standard: Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
- Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
- Implementation specifications:**
 - Disposal (*Required*). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

MB&F Note: Simply pressing the “Delete” key may not be sufficient to completely destroy electronic protected health information. Additional software (or physical destruction) may be required.

- Media re-use (*Required*). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
- Accountability (*Addressable*). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
- Data backup and storage (*Addressable*). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

TECHNICAL SAFEGUARDS (45 C.F.R. § 164.312)

- Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as described above.
- Implementation specifications:**
 - Unique user identification (*Required*). Assign a unique name and/or number for identifying and tracking user identity.
 - Emergency access procedure (*Required*). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
 - Automatic logoff (*Addressable*). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

- Encryption and decryption (*Addressable*). Implement a mechanism to encrypt and decrypt electronic protected health information.

MB&F Note: These implementation specifications—like other provisions of the Security Rules—can lead to uncertainty. For example, suppose a computer system has an automatic logoff feature. After how many minutes should the feature activate? One minute? Ten minutes? Twenty minutes? There is no clear answer. Presumably, a shorter period should be chosen if the computer is easily accessible to unauthorized personnel. On the other hand, if the computer is located in a secured area, the logoff feature could, presumably, activate after a longer period of time.

- Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
 - Implementation specification:** Mechanism to authenticate electronic protected health information (*Addressable*). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
- Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
 - Implementation specifications:**
 - Integrity controls (*Addressable*). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
 - Encryption (*Addressable*). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

ORGANIZATIONAL REQUIREMENTS (45 C.F.R. § 164.314)

- Standard: Business associate contracts or other arrangements.**
 - The contract or other arrangement between the covered entity and its business associate must meet the applicable Implementation Specification described below.
 - A covered entity is not in compliance with the standards regarding disclosures of protected health information to business associates and this standard if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
 - Terminated the contract or arrangement, if feasible; or
 - If termination is not feasible, reported the problem to the Secretary.
- Implementation specifications (*Required*).**
 - Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will—
 - Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;
 - Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
 - Report to the covered entity any security incident of which it becomes aware;
 - Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.
 - Other arrangements.
 - When a covered entity and its business associate are both governmental entities, the covered entity is in compliance if--
 - It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of the business associate contract requirements; or
 - Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of the business associate contract requirements.

- If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the business associate contract requirements, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by the business associate contract requirements, and documents the attempt and the reasons that these assurances cannot be obtained.

- The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

- Standard: Additional rules for group health plans.** Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to the enrollment/disenrollment information exception, the exception to obtain premium bids, the exception for information necessary to modify or terminate the plan, or as a permitted disclosure authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

- Implementation specifications (*Required unless exception above applies*).** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—
 - Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;
 - Ensure that the adequate separation is supported by reasonable and appropriate security measures;
 - Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
 - Report to the group health plan any security incident of which it becomes aware.

SECURITY SAFEGUARDS UNDER PRIVACY REGULATIONS (45 C.F.R. § 164.530(c))

- Standard: Safeguards.** A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

MB&F Note: This standard applies not just to electronic protected health information. Rather, it applies to all protected health information.

Administrative Safeguards.

Administrative safeguards include items such as:

- Appointing a Privacy Official and contact person;
- Creating a policy that work stations must be regularly cleared (e.g., clean off a desk at night so night personnel will not be able to see the information);
- Verifying that off-site storage companies have adequate safeguards;
- When returning information from off-site location, request box and not individual file or claim;
- Providing appropriate workforce training;
- Including return address on outside of envelope if inside materials contain protected health information;
- Mark internal envelopes “Confidential”. Also consider using sealed envelopes;
- Faxes should be marked “Confidential” and handled by a trained individual;
- Implementing policies and procedures for use/disclosure of protected health information;
- Drafting a privacy notice and authorizations; and
- Drafting and executing business associate agreements.

Technical Safeguards.

Technical safeguards include items such as:

- Limiting access to protected health information by creating computer firewalls;
- Limiting access to protected health information by using timed screen saver/automatic log-off; and
- Limiting access to protected health information by requiring computer password and authentication.

Physical Safeguards.

Physical safeguards include items such as:

- Protecting access to, or disclosure of, protected health information by locking protected health information in file cabinets;
- Protecting access to, or disclosure of, protected health information by locking offices, limiting access to work areas, storage spaces, desks and lockers; and
- Protecting access to, or disclosure of, protected health information by restricting access to work areas by visitors.

Appendix A

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervisions	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or other Arrangement	(R)

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

X:\CLIENTB\072238\0001\A0573637.1