Health Insurance Portability and Accountability Act (HIPAA)

BUSINESS ASSOCIATES

The Health Insurance Portability and Accountability Act (HIPAA) improves the efficiency and effectiveness of the health care system by promoting electronic data exchanges of health information while protecting individuals' privacy. HIPAA has been called the most sweeping piece of healthcare legislation since Medicare. The American Recovery and Reinvestment Act (Stimulus Bill) signed into law on February 17, 2009 dramatically expanded the scope and enforcement of HIPAA. "Business associates" that provide services to "covered entities" such as health care providers, health plans and health care clearinghouses are now directly regulated under certain provisions of HIPAA.

The Administrative Simplification provisions of HIPAA required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information (ePHI). The HIPAA Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of ePHI. The primary objective of the Security Rule is to protect the confidentiality, integrity, and availability of ePHI when it is stored, maintained, or transmitted. The standards in the Security Rule mirror generally accepted best practices for managing an information technology organization and a company's information technology resources. The security standards are generally consistent with other leading security frameworks, such as the ISO 17799 security standards.

The Security Rule is divided into three groups: administrative, physical and technical safeguards. Administrative safeguards make up 50% of the Security Rule's standards. They require documented policies and procedures for managing day-to-day operations, the conduct and access of workforce members to ePHI, and the selection, development, and use of security controls. The administrative safeguards are further divided into 9 categories with 23 standards. The physical safeguards are a series of requirements meant to protect ePHI systems and ePHI from unauthorized physical access. Individuals and businesses must limit physical access while permitting properly-authorized access. The physical safeguards are further divided into 4 categories with 10 standards. The technical safeguards impose requirements for using technology to protect ePHI, particularly controlling access to it. The technical safeguards are divided into 6 categories with 10 standards. The standards are delineated into either required or addressable implementation specifications. Compliance with these standards by business associates is required by February 17, 2010.

Compliance with the Security Rule requires a coordinated effort among the various constituents of any organization that provides services to covered entities as a business associate. The following check list is intended to serve as a work plan by which a business associate can meet the HIPAA Security Rule requirements.

HIPAA Security Checklist

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
		ADMINISTRATIVE SAFEGUARDS			
Security Management Process:	164.308(a)(1)(i)	**Policies and Procedures:** Implement policies and procedures to prevent, detect, contain and correct security violations.			
	164.308(a)(1)(ii)(A)	**Risk Analysis:** Conduct an organization- wide analysis of the services offered, assessing risks and the likelihood that a risk will occur in accordance with IAW NIST Guidelines (R)			
	164.308(a)(1)(ii)(B)	**Risk Management**: For each risk assessed in the risk analysis, implement controls to manage the risks in accordance with IAW NIST Guidelines (R)			
	164.308(a)(1)(ii)(c)	**Sanction Policy:** Develop policies and procedures to secure ePHI. Define sanctions to be imposed when a member of the workforce violates these policies and procedures. (R)			
	164.308(a)(1)(ii)(D)	**Information System Activity Review:** Implement procedures to regularly audit and review records of IS activity and IT systems, including audit logs, incident reports, access reports, security controls (i.e., password management, to backup/restore, disaster recovery, software installation and configuration, etc.). (R)			
Assigned Security Responsibility:	164.308(a)(2)	**Privacy Officer:** Identify a security officer to be responsible for the development and implementation of the policies and procedures; understand HIPAA laws and regulations; establish appropriate levels of oversight; support education, awareness and hotline reporting activities; conduct periodic HIPAA risk assessments; participate in the development of corrective action plans and mitigation strategies for identified security risks; and tract progress and ensure risks are appropriately communicated to senior management and the board.			
Workforce Security:	164.308(a)(3)(i)	**Policies and Procedures**: Implement policies and procedures to ensure that all members of the workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to ePHI.			
	164.308(a)(3)(ii)(A)	**Authorization and Supervision:** Implement procedures for the authorization and/or supervision of employees who work with ePHI in all locations where it might be accessed to ensure data integrity. (A)			

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
	164.308(a)(3)(ii)(B)	**Workforce Clearance Procedures**: Implement procedures to ensure that workforce access is appropriate based on job duties. Workforce managers must review what each member of the workforce is authorized to view or access. There must be an audit mechanism that identifies who accesses what data. (A)			
	164.308(a)(3)(ii)(C)	**Termination Procedures:** Implement procedures to prevent ePHI access after a member of the workforce is terminated, such as the return of accounts, keys, badges, portable devices, etc.			
Information Access Management:	164.308(a)(4)(i)	**Policies and Procedures:** Implement policies and procedures for authorizing access to ePHI.			
	164.308(a)(4)(ii)(A)	**Isolating Healthcare and Clearinghouse Functions:** Healthcare and clearinghouse functions within a single organization must be separated. Clearinghouse function access is role based and limited to members of the workforce with clearinghouse job duties. If a clearinghouse is part of a larger organization, policies and procedures must be implemented to protect ePHI from the larger organization. (A)			
	164.308(a)(4)(ii)(B)	**Access Authorization:** Implement policies and procedures to address how workstations, transactions, programs, etc. where ePHI resides are accessed by users. (A)			
	164.308(a)(4)(ii)(C)	**Access Establishment and Modification.** Implement policies and procedures for the periodic review and documentation of user permission for rights of access to a workstation, transaction, program, or process. Modify user permissions as necessary to secure ePHI. (A)			
Security Awareness & Training:	164.308(a)(5)(i)	**Security Training Programs**: Implement a security awareness and training program for all members of the workforce (including management).			
	164.308(a)(5)(ii)(A)	**Security Reminders**: Create screensavers, posters, in-service training and communications to ensure that all employees, from management to support staff, understand their role in securing ePHI. (A)			
	164.308(a)(5)(ii)(B)	**Protection from Malicious Software:** Implement policies and procedures to evaluate and use new software, protect bootable drives, corporate anti-virus procedures, firewalls, intrusion detection, etc. (A)			
	164.308(a)(5)(ii)(C)	**Login Monitoring:** Implement policies and procedures for monitoring login attempts (internal and external) and to detect, review and report violations. (A)			

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
	164.308(a)(5)(ii)(D)	**Password Management:** Implement policies and procedures for password management, i.e., aging, complexity, communication of passwords, storage, temporarily disabling accounts after a pre-determined number of unsuccessful logins, discouraging users from writing down passwords, disallowing use of previous passwords, etc. (A)			
Security Incident Procedures:	164.308(a)(6)(i)	**Policies and Procedures**: Implement policies and procedures to address security incidents.			
	164.308(a)(6)(ii)	**Response and Reporting**: Implement policies and procedures for responding to, and reporting security incidents: incident handling, preparation, identification, containment, eradication, recovery, "lessons learned" and to mitigate to the extent practicable, harmful effects of known security incident and document incidents and their outcomes. (R)			
Contingency Plan:	164.308(a)(7)(i)	**Policies and Procedures:** Establish 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 ePHI.			
	164.308(a)(7)(ii)(A)	**Data Backup Plan**: Implement policies and procedures for data backup to ensure all critical ePHI is identified and included in the plan. Provide for periodic testing backup restore, rotation, retention and offsite storage with appropriate access restrictions. (R)			
	164.308(a)(7)(ii)(B)	**Disaster Recovery Plan**: Implement policies and procedures to restore loss of data from backup media, including operating systems, subsystems, utilities and applications. (R)			
	164.308(a)(7)(ii)(C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of the organization's critical business processes for the protection and availability of ePHI in the event of a disaster, including platforms, applications, data, networks, support services, voice, websites, etc. (R)			
	164.308(a)(7)(ii)(D)	**Testing and Revision Procedures:** Implemented procedures for the periodic testing and revision of the contingency plans. (A)			
	164.308(a)(7)(ii)(E)	**Application and Data Criticality Analysis**: Conduct a business impact analysis mapping critical clinical processes to associated applications, data, IT, infrastructure components, and support services so as to identify internal, external and processing dependencies and minimize recovery resources to recover ePHI. (A)			

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
Security Evaluation:	164.308(a)(8)	**Security Evaluation.** Implement ongoing periodic technical evaluations to determine the extent to which security policies and procedures meet ongoing requirements of the HIPAA Security Rule. (R)			
Business Associate Contracts and Other Arrangements:	164.308(b)(1)	A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguards the information.			
	164.308(b)(4)	**Written Business Associate Agreements:** Written contracts are required between an organization and its business associates that meet the applicable requirements of Sec. 164.314(a) and authorize termination of the business associate agreement if the situation warrants. Ensure that business associates implement controls to maintain the privacy and security of ePHI. Notify the Department of Health and Human Services if business associates do not maintain the requirements of the Security Rule. (R)			

PHYSICAL SAFEGUARDS

Facility Access Controls:	164.310(a)(1)	**Policies and Procedures**: Implement policies and procedures to limit physical access to ePHI systems and ePHI data.			
	164.310(a)(2)(i)	**Contingency Operations:** Implement policies and procedures to limit physical access to ePHI systems and the facilities in which systems are housed, with properly authorized access to members of the workforce and vendors after a disaster. (A)			
	164..310(a)(2)(ii)	**Facility Security Plan.** Implement policies and procedures to safeguard facilities and equipment from unauthorized physical access, tampering, and theft of information, including perimeter, public, private and restricted areas. (A)			
	164.310(a)(2)(iii)	**Access Control and Validation Procedures**: 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. Maintain audit trails of access. (A)			
	164.310(a)(2)(iv)	**Maintenance Records**. Implement policies and procedures to document repairs and modifications to the physical components of a facility and to IT systems which are related to security (for example, hardware, walls, doors, and locks)(A)			

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
Workstation Use:	164.310(b)	**Policies and Procedures: I**mplement policies and procedures that specify the proper functions of a workstation environment, how those functions are to be carried out and the physical attributes of the environment surrounding the workstations on which ePHI is housed or processed. Note. Workstation is defined to include public workstations, servers, laptops, desktops, handheld devices, image scanners, network devices, etc. (R)			
	164.310(c)	**Workstation Security**. Implement physical safeguards for all workstations on which ePHI is viewed or updated to restrict access to authorized users only. (R)			
Device and Media Controls:	164.310(d)(1)	**Policies and Procedures:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within a facility.			
	164.310(d)(2)(i)	**Disposal**: Implement policies and procedures for the sale, transfer, or final disposition of all electronic media that processes ePHI, (hardware) or electronic media on which it is stored to ensure confidentiality. (R)			
	164.310(d)(2)(ii)	**Media Reuse**: Implement procedures for the removal of all traces of ePHI from electronic media before the media are available for reuse. Focus on all possible re-use in and out of the organization as well as movement with the organization. (R)			
	164.310(d)(2)(iii)	**Accountability**: Maintain inventory control of all equipment and media movement on which ePHI is accessed or updated. Develop an audit trail of who has access to this equipment, including responsible users and technical staff in charge of maintenance and repair for members of the workforce and vendors. (A)			
	164.310(d)(2)(iv)	**Data Backup and Storage**: Create and maintain retrievable, mirrored, backup copies of ePHI and document the backup process to ensure information system architecture changes and equipment moving do not jeopardize the availability of data. (A)			
TECHNICAL SAFEGUARDS					
Access Controls:	**164.312(a)(1)**	**Policies and Procedures:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access to only those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).			

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
	164.312(a)(2)(i)	**Unique User Identification:** Implement policies and procedures to validate a user's identity, i.e, validate that a user who wants access is indeed who that person says he/she is by checking his/her ID papers. Implement controls for unique user ID that is auditable and traceable. (R)			
	164.312(a)(2)(ii)	**Emergency Access Procedure:** Maintain procedures so t hat if a person needs access to data due to an emergency, he/she will be allowed access, with a log (video camera) that records every piece of information that the person accesses or modifies. Undertake post-facto log review to ensure that the person adhered to emergency access policies. (R)			
	164.312(a)(2)(iii)	**Automatic Logoff:** Implement controls to ensure IT systems log users off after a predetermined period of inactivity. (A)			
	164.312(a)(2)(iv)	**Encryption and Decryption:** Implement controls to ensure confidentiality of ePHI during electronic transmission and users' credentials stored on networks to prevent compromising data integrity. (A)			
Audit Controls:	**164.312(b)**	**Audit Controls:** Implement audit mechanisms (hardware, software, procedural) to record and examine system activity. Create audit rules: user account activity audits through automated audit controls; activate appropriate security features to ensure user access accountability; access and modification of sensitive or critical files is logged; access to logs is restricted; audit trails include sufficient information to tract activity back to user; hardware fault controls are logged to indicate all detected errors and determine of recovery from the malfunction is feasible. (R)			
Integrity	**164.312(c)(1)**	**Mechanism to Authenticate ePHI:** Implement controls to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. (A)			
Person or Entity Authenticate	164.312(d)	**Person or Entity Authentication**: Implement controls to confirm that the user or system is indeed who they claim to be to protect ePHI from unauthorized changes or disclosure. Need to know, e.g., passwords, PINs, client/server handshake, small cards or other tokens, drivers licenses, secret words, challenge-response, such as call- back verification, biometrics, single sign-on, etc. Disallow shared IDs internally or by vendors or other third parties. (R)			
Transmission Security	**164.312 (e)(1)**	Policies and Procedures: Guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.			
	164.312(e)(2)(i)	**Integrity Controls:** Implement controls to protect against message tampering during e-PHI communications across networks (ensure message sent= message received). (A)			

STANDARD	HIPAA SECURITY RULE REFERENCE	IMPLEMENTATION SPECIFICATION (R) = REQUIRED (A) = ADDRESSABLE	Assigned Team	Implement Solution	Status
	164.312(e)(2)(ii)	**Encryption:** Where appropriate, implement encryption controls. (A)			
Policies and Procedures Documentation Requirements		**Policies and Procedures Documentation Requirements**: All policies and procedures to safeguard ePHI must be documented along with policy changes. Documentation must be kept for 6 years and be open for review. **Security Policies and Documents:** • Authentication Standards • E-mail and use of ePHI • Remote Access-Tech Security Practices and Procedures • Workstation Use and Security • Disposal/destruction/Reuse of e-PHI • Security Incident Report (Disaster Recovery) • IT Infrastructure-System Standards • Data Back-Up (Disaster Recovery) • Auditing of Access to e-PHI • Retention of e-mail transmissions • Portable Devices-Use and Security • Non-IT System Administrator Role, Access Controls, Etc. • Data Center Security • IT System Administrator Role, Access Controls, Etc. • System Change Management • Auditing of Access to ePHI			

Butzel Long's Health Care Industry Group

Robert H. Schwartz	schwartzrh@butzel.com	248 258 2611
Susan H. Patton	patton@butzel.com	734 213 3432
Carol A. Romej	romej@butzel.com	734 302 1025
Julie A. Rajzer	rajzer@butzel.com	248 258 2610
Thomas L. Sparks	sparks@butzel.com	517 372 4372
Max R. Hoffman	hoffman@butzel.com	517 372 4374

BUTZEL LONG
ATTORNEYS AND COUNSELORS

www.butzel.com