

Two HIPAA Deadlines Fast Approaching

Security Rule - Deadline for Small Health Plans April 20, 2006

An employer sponsoring a group health plan that creates, maintains, or transmits protected health information through electronic media must comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (“the Rule”). The compliance deadline for small health plans (those with annual receipts under \$5 million) is April 20, 2006.¹ Large health plans were to comply by April 20, 2005.

The Rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards surrounding electronically formatted protected health information (E-PHI), such as maintained under a group health plan. There are four general security requirements a covered entity must meet:

1. Ensure confidentiality, integrity and availability of all E-PHI that the covered entity creates, receives, maintains or transmits,
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information,
3. Protect against any reasonably anticipated uses or disclosures that are not permitted or required by the privacy regulations, and
4. Ensure the compliance of its workforce.

The Rule requires covered entities to establish policies and procedures to comply with standards and implementation specifications set forth under the rule. Standards set the minimum level of security that must be met by covered entities. The standards are implemented through either “required” or “addressable” implementation specifications. A covered entity must comply with all required implementation specifications. Addressable implementation specifications must be implemented if they are reasonable and appropriate for the group health plan. If it is determined that the addressable specification is not reasonable or appropriate, then the covered entity must document why and provide a reasonable alternative. It is critical that the employer document that the plan complies with each standard and implementation specification. Failure to do so may result in legal ramifications.

The Rule requires, among other things, that the plan appoint a security officer, conduct a HIPAA security risk assessment, develop policies and procedures in handling E-PHI, and conduct training of the workforce. Following are the standards and implementation procedures as outlined under the regulation:

¹ Receipts are defined as:

- 1) Fully Insured: the amount of total premiums paid for health insurance in the plan’s last full fiscal year.
- 2) Self Insured: total amount of paid for health care claims during the plan’ last full fiscal year. Claims paid by the employer, plan sponsor or benefits fund, whichever is applicable.
- 3) Self Insured and Insured Options: plans that provide health benefits through a mixture of purchased insurance and self insurance should combine the total premiums paid and the total paid for health care claims in the plan’s last full fiscal year.

Standards	Sections	Implementation Specifications (R) = required, (A) = Addressable
Administrative Safeguards*		
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 Supervision (A) Workforce Clearance Procedure 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)
Evaluation	164.308(a)(8)	Application & Data Criticality Analysis (R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards*		
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*		
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)
Policies and Procedures and Documentation Requirements**		
Policies and Procedures	164.316(a)	(R)
Documentation	164.316(b)	(R)
Organizational Requirements**		
Amend Plan Documents	164.314(b)	(R)

* "Appendix A to Subpart C of Part 164- Security Standards: Matrix," 68 Federal Register 34 (20 February 2003), pp.8380.

**45 CFR 164.316, 45 CFR 164.314

You can view the regulations in their entirety at:

<http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>.

If you need additional assistance to comply with HIPAA security requirements Agent 77, a developer of tools to assist HR with administration, compliance, and training, offers a HIPAA compliance tool. The HIPAA Now Toolkit is a narrated CD that covers the employer HIPAA compliance process step by step, beginning from determining whether or not a company is a “covered entity”, through all of the checklists, job descriptions and forms necessary to be in compliance.

HIPAA Now Toolkits are available through Kibble & Prentice. Please contact Kellie Stone at 206-441-6300 or kellie.stone@kpcom.com if you are interested in purchasing this tool.

HIPAA Privacy Notice Mailing - Large Health Plans April 14, 2006

HIPAA privacy rules require a health plan to provide a reminder about their privacy notice and how to obtain the notice at least once every three years. Large health plans must distribute a reminder by April 14, 2006, if they have not already done so at an earlier time. A large health plan is defined by having annual receipts in excess of \$5 million. The initial privacy notice deadline for large health plans was April 14, 2003. Health and Human Services (HHS) provided guidance as to the plan sponsor’s flexibility in providing this notice. A plan sponsor may:

1. Resend the full Notice of Privacy Practices (NPP);
2. Mail a separate reminder regarding the NPP availability and how to obtain a copy; or
3. Include this information “in a plan-produced newsletter or other publication.”

(HHA FAQ March 6, 2006). <http://www.hhs.gov/ocr/hipaa/>

Small health plans have until April 14, 2007, to comply with the above notice requirement.