AdvantEdge PERFORMANCE THAT MATTERS

HIPAA Checklist

HIPAA and HITECH require physician practices and hospitals to have procedures in place to deal with specific aspects of PHI (Protected Health Information) including disclosures, access and security. Major components are the Privacy Rule[1], the Security Rule[2] and the Breach Notification Rule[3]. This checklist provides an overview of the requirements. A companion worksheet is available on the AdvantEdge website and upon request.

More detail is available in the official HHS documents and the AdvantEdge Compliance Office is available to assist clients in any of these areas.

Privacy Rule

The Privacy Rule applies to all media types including paper, oral, and electronic. It requires organizations to consider the confidentiality, integrity, and availability of PHI and to have procedures in place to address the use and disclosure of PHI, notice of privacy practices, and minimum necessary approach to using PHI.

Business Associate Agreements	Are BAA's in place with every entity that has access to your PHI?	
Staff Awareness and Training	Does everyone know the definition of PHI? Are they aware of the restrictions on its use? Do they know permitted uses and disclosures? Is there an official training program?	
Administrative Requirements	Do you have written policies and procedures? A designated Privacy Official? Compliant procedures? Record retention policies? Do you have policies in place for proper PHI disposal? Paper and electronic?	

Security Rule

The HIPAA Security Rule requires appropriate Administrative, Physical, and Technical Safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

Physical Safeguards	Is your office/hospital location secure? Is computer equipment protected from unauthorized users? Are portable devices (laptops, phones) equipped with passwords and encryption?	
Administrative Safeguards	Do you have a designated Security Official? When was the last security assessment (risk analysis)? How often are they scheduled? Procedures to limit access to information?	
Technical Safeguards	Controls on access to systems? Measures to prevent improper changes to patient data? Secure passwords? Data encryption? Data backups? Do you have a **tested** disaster recovery plan?	

For more details, the Indian Health Service has prepared a detailed HIPAA Security Checklist[4].

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

[4] http://www.ihs.gov/hipaa/documents/ihs_hipaa_security_checklist.pdf

Breach Notification Rule

Healthcare providers and their business associates are required to provide full disclosure about a breach. Any instance where PHI has been compromised and is in the position to be used in a harmful manner is considered a breach.

Breach identification	Are employees trained to identify and report a potential breach? Is a risk assessment process in place to determine potential harm of any breach? Do you have a designated person to handle any suspected or identified breach? Are procedures in place to document all potential breaches?	
Notifications	Do you have procedures in place to report a breach? Is your process able to report specified breaches to HHS and the media? Is there a designated process to report a breach among business associates and the covered entity? Is your process able to provide notifications within the required timeframe?	

Background

The use of health information technology continues to expand in health care. Although these new technologies provide many opportunities and benefits for consumers, they also pose new risks to consumer privacy. Because of these increased risks, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) include national standards for the privacy of protected health information, the security of electronic protected health information, and breach notification to consumers. HITECH also requires HHS to perform periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules.[5]

- The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards
- The protocol covers requirements for the Breach Notification Rule.

Each healthcare organization is expected to have “reasonable and appropriate administrative, physical and technical safeguards that are tailored to the size and complexity of your organization”.[6]

[5] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/

[6] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SecurityRiskAssessment_FactSheet_Updated20131122.pdf