E COM SECURITY® SOLUTIONS

HIPAA Compliance Assessment and Attestation

Strengthen security postures and identify weaknesses with a consultative risk assessment while navigating the complex HIPAA compliance landscape.

About HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) states that information in any form – oral, paper, or electronic – that relates to a specific individual is protected health information, or PHI and requires that covered entities ensure confidentiality, integrity and availability of all electronic PHI; that they anticipate information security threats, both intentional and unintentional; and that they ensure workforce compliance.

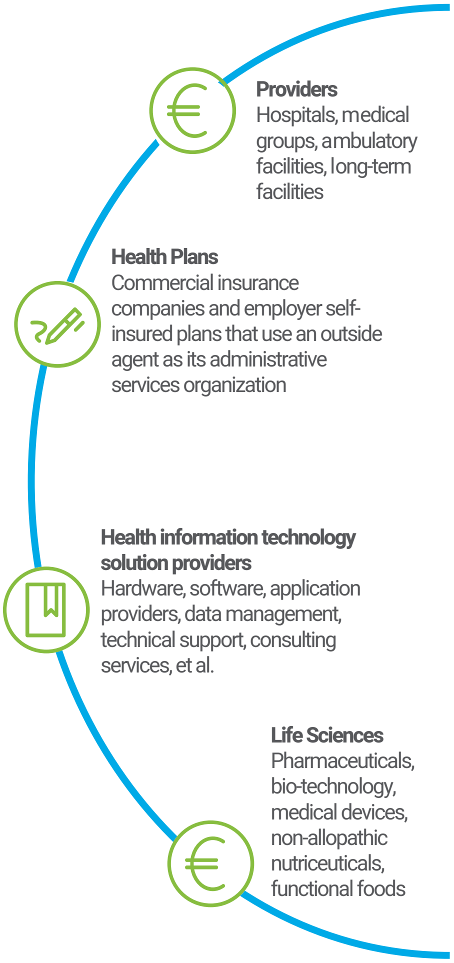
Privacy and Security in Health Care

The health care industry is particularly susceptible to data fraud and medical identity theft due to the nature and content of the data it creates, collects, and stores. Sensitive data such as SSNs, insurance identification numbers, payment information, and medical provider identification numbers enables criminals to file fraudulent claims that often go undetected for long periods of time. The organizational consequences of data breaches can be significant: monetary penalties, damage to reputation, and lost revenues are most notable. The move toward an entirely automated health care system featuring electronic and personal health records (EHRs and PHRs), clinical data warehousing, and increased transparency means more data is at risk and suggests an urgent review of privacy and security policies and procedures.

Privacy and security: hot spots

Increased use of automated technologies (i.e., e-prescribing, billing, medical claims processing, EHRs, and PHRs) and gravitation toward local and national health information exchanges (HIEs) have expanded the health care privacy and security landscape. Electronic exchange of patient information offers greater convenience and efficiency in health care delivery, but not without greater data risk and liability due to broader access. For example, patient information exchanged via PHRs, social media networks (i.e., Facebook, Twitter), and mobile devices is subject to HIPAA regulations. To optimize the utility of health information technology (HIT), effective exchange of data between sectors (i.e., provider groups, diagnostic laboratories, health plans, public health agencies, financial institutions, etc.) is essential. This broader exchange, however, further distributes privacy and security risks and increases the likelihood of data breaches.

Covered Entities



Providers
Hospitals, medical groups, ambulatory facilities, long-term facilities

Health Plans
Commercial insurance companies and employer self-insured plans that use an outside agent as its administrative services organization

Health information technology solution providers
Hardware, software, application providers, data management, technical support, consulting services, et al.

Life Sciences
Pharmaceuticals, bio-technology, medical devices, non-allopathic nutriceuticals, functional foods

For more information

Visit www.ecomsecurity.org or E-Mail us at sales@ecomsecurity.org.

Assessing health care organization security and privacy preparedness

E Com Security Solutions' help organizations from current and emergent privacy and security challenges in health care, as well as preparedness measures to avoid risk. A basic approach to assessing an organization's current preparedness requires consideration in three key areas

Strategy	Objective	Benefit	Examples
Risk Management	Identify and assess data security risks to develop appropriate security controls to mitigate or avoid risk	Allows health care organizations to make informed decisions on how to allocate security resources to improve data protection	• Assess current security controls, audit logs, and current policies and procedures • Review current Business Associate Agreements (BAA)
Security and Privacy Program	Develop and implement policies, procedures, and training needed to mitigate or avoid risk	Creates baseline standards for the secure handling of sensitive patient information; creates organization-wide awareness of data privacy and security policies	• Create policies for proper handling of sensitive data; notifying HHS and the media of data breaches • Train employees on data handling policies and apply policies to systems that store sensitive data • Ensure employees are aware of data handling procedures and notification policies through effective training • Modify BAAs to prevent breaches and ensure liability in event of breach • Implement safeguards such as data encryption, user- and role-based access and identity management to prevent and limit inappropriate access to PHI • Protect information assets and manage data associated risks through an accepted security framework (i.e., HITRUST)
Compliance	Validate effective risk management and governance	Reduces organizational risk; creates customer trust and confidence in an organization's protection of PHI; reduces potential for financial penalties due to reasonable cause or willful neglect	• Demonstrate development and implementation of policies to address identified risks • Monitor and log data handling procedures and compliance with established policies • Conduct regular internal and third-party security audits and compare reports to internal and external benchmarks that may exist

E COM SECURITY® SOLUTIONS

E Com Security Solutions' provide Compliance, Application Security, Infrastructure security and advisory services through the cloud, managed security services and software that help clients protect their most important assets from evolving cyber threats. As the global professional services and consulting network, with approximately 300 security consultants world wide, we bring world-class capabilities and high-quality services to our clients.