



Global DataGuard

PREDICT AND PROTECT

HIPAA COMPLIANCE



**ACHIEVING HIPAA COMPLIANCE WITH
MANAGED SECURITY SERVICES**

Achieving HIPAA Compliance with Managed Security Services

The Health Insurance Portability and Accountability Act (HIPAA) requires that the Department of Health and Human Services (HSS) establish national standards to address the security and privacy of healthcare data and electronic healthcare transactions, as well as provide national identifiers for providers, health plans and employers. Its primary goal is to simplify the administrative processes of the healthcare system and to protect patient privacy.



To help healthcare organizations comply with privacy requirements, the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” commonly known as the Security Rule, has been adopted in order to implement the various provisions of HIPAA. In general, Covered Healthcare Providers, Health Plans, and Healthcare Clearinghouses must comply with the standards, requirements and implementation specifications of the HIPAA Security Rule. This final rule specifies a series of administrative, physical, and technical security procedures for covered entities to use to assure the confidentiality of Electronic Protected Health Information (EPHI). The Security Rule defines these safeguard as follows:

- **Administrative Safeguards** – these are the administrative actions, policies and procedures designed to manage the selection, development, implementation and maintenance of security measures that protect electronic health information. These safeguards also manage the conduct of the covered entity’s workforce in relation to the protection of said information. The Administrative Safeguards comprise over half of the HIPAA security requirements and compliance with these safeguards require an evaluation of security controls already in place, accurate and thorough risk analysis, and a series of documented solutions derived from factors that are unique to each covered entity.
- **Physical Safeguards** – these are the physical measures, policies and procedures designed to protect a covered entity’s electronic information systems, related buildings and equipment from natural and environmental hazards, as well as unauthorized intrusion. When evaluating and implementing these safeguards, a covered entity must consider all physical access to EPHI beyond an actual office, such as work force members’ homes or other physical locations where they might access EPHI.
- **Technical Safeguards** – these safeguards cover the technology and the policies and procedures associated with its use that protect EPHI and control access to it. Technical safeguards are becoming more important as healthcare organizations are faced with the challenge of protecting EPHI from various internal and external threats. Based on the fundamental concepts of flexibility, scalability and technology neutrality, these safeguards allow a covered entity to determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.

Compliance with these security standards, as defined by HIPAA, is imperative to the ongoing business operations of healthcare companies. Failure to comply may result, not only in regulatory sanctions and fines, but also direct business loss as a result of lawsuits, damage to an organization’s reputation and degradation of the public’s trust.

Global DataGuard offers a full suite of enterprise-class products and services to assist healthcare organizations in successfully implementing the Security Standards outlined by HIPAA. Our extensive experience in fully integrated “no gaps” network security solutions and world-class Managed and Professional Services can help improve an organization’s security and HIPAA-compliance posture while significantly reducing security infrastructure costs. The chart below shows how Global DataGuard’s Managed Security Services and Professional Services align directly with these HIPAA Security Standards. The implementation specifications identified in this chart are additional detailed instructions for implementing a particular standard. If a specification is required (R), the covered entity must implement policies and/or procedures that meet what the implementation specification requires. If a specification is addressable, (A), then the covered entity must assess whether it is a reasonable and appropriate safeguard within that particular organization’s environment.



ADMINISTRATIVE PROCEDURES

ADMINISTRATIVE SAFEGUARDS

Standard	Summary of Requirements	Solutions
Security Management Process 164.308 (a) (1)	<p>R = Required; A = Addressable</p> <p>This standard states that covered entities must implement policies and procedures to prevent, detect, contain and correct security violations.</p> <p>There are four implementation specifications in the Security Management Process standard. These include:</p> <ul style="list-style-type: none">• Risk analysis (R)• Risk management (R)• Sanction policy (R)• Information system activity review (R)	<p>Global DataGuard's Professional Services team can help you evaluate your security management process and make recommendations for areas in need of improvement in relation to HIPAA requirements.</p> <p>Additionally, our Managed Firewall and Network Access Monitoring services can provide you with 24x7 firewall management and monitoring of your network access points by certified security professionals. Our firewall experts will audit policies and procedures to ensure that they align with HIPAA requirements, perform on-going rule-set changes and monitor these devices for any signs of attack.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Firewall Management & Monitoring• Log Management & Monitoring• Managed Intrusion Prevention and Detection• Network Access Monitoring• Threat Management™• Professional Services
Workforce Security 164.308 (a) (3)	<p>This standard states that covered entities must implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (EPHI) and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.</p> <p>There are three implementation specifications in the Workforce Security standard. These include:</p> <ul style="list-style-type: none">• Authorization and/or supervision (A)• Workforce clearance procedure (A)• Termination procedures (A)	<p>Global DataGuard can help you to define secure boundaries to manage and monitor access to information and applications across multiple systems and disciplines. Simply put, our network access control and monitoring capabilities can easily and intelligently define who can access information, from which locations, and at what times. If anyone attempts to violate these boundaries, you'll be immediately alerted.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Network Access Control & Monitoring• Log Management & Monitoring• Professional Services

Standard	Summary of Requirements	Solutions
<p>Information Access Management 164.308 (a) (4)</p>	<p>This standard states that covered entities must implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of the Privacy Rule (subpart E).</p> <p>There are three implementation specifications in the Information Access Management standard. These include:</p> <ul style="list-style-type: none"> • Isolating health care clearinghouse functions (R) • Access authorization (A) • Access establishment and modification (A) 	<p>Global DataGuard’s world-class Professional Services team will work with you to establish information access procedures, set user access privileges, and conduct regular account reviews. Our Enterprise UTM solution will help you to cost-effectively define and monitor your corporate security posture, striking the right balance between easy, efficient access for authorized users and uncompromising security.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Network Access Control & Monitoring • Log Management & Monitoring • Professional Services
<p>Security Awareness and Training 164.308 (a) (5)</p>	<p>This standard states that covered entities must implement a security awareness and training program for all members of its workforce, including management.</p> <p>There are four implementation specifications in the Security Awareness and Training standard. These include:</p> <ul style="list-style-type: none"> • Security reminders (A) • Protection from malicious software (5A) • Log-in monitoring (A) • Password management (A) 	<p>Global DataGuard will help you evaluate your current program in key areas such as policy, process, people and products, and will provide a security program roadmap to help you ongoing HIPAA compliance in conjunction with the Security Awareness and Training standard.</p> <p>In addition, we can help you easily manage the relationships between employees, customers, business partners and all the disparate applications and systems that they depend on.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Data Leakage Monitoring • Log Management & Monitoring • Network Access Control & Monitoring • Professional Services



Standard	Summary of Requirements	Solutions
Security Incident Procedures 164.308 (a) (6)	<p>This standard states that covered entities must implement policies and procedures to address security incidents. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.</p> <p>There is one implementation specification in the Security Incident Procedures standard. It includes:</p> <ul style="list-style-type: none">• Response and reporting (R)	<p>Global DataGuard's behavioral-based Enterprise UTM security suite and Managed Security Services will enable you to proactively identify, classify and respond to security incidents.</p> <p>Our certified security professionals can provide 24x7 enterprise-wide security monitoring and management of your network. We can assist you with actionable, event-based remediation, as well as incident response and on-demand reporting to help you identify and prevent network security problems and respond to immediate security issues.</p> <p>Further, our log management and monitoring capabilities will continuously monitor log files for attack signatures and alerts, notify you of any anomalies, and provide you with 24/7 access to online summary reports.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Firewall Management & Monitoring• Log Management & Monitoring• Data Leakage Monitoring• Managed Intrusion Prevention and Detection• Network Access Control & Monitoring• Threat Management™• Professional Services
Contingency Plan 164.308 (a) (7)	<p>This standard states that covered entities must establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI.</p> <p>There are five implementation specifications in the Contingency Plan standard. These include:</p> <ul style="list-style-type: none">• Data backup plan (R)• Disaster recovery plan (R)• Emergency mode operation plan (R)• Testing and revision procedures (A)• Applications and data criticality analysis (A)	<p>Our Professional Services team can work with you to develop a Contingency Plan and ensure that it meets or exceeds minimum HIPAA requirements for procedures, reporting and response as indicated by this standard.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Professional Services

PHYSICAL SAFEGUARDS

Standard	Summary of Requirements	Solutions
<p>Facility Access Controls 164.310 (a) (1)</p>	<p><i>R = Required; A = Addressable</i></p> <p>This standard states that covered entities must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.</p> <p>There are four implementation specifications in the Facility Access Controls standard. These include:</p> <ul style="list-style-type: none"> • Contingency operations (A) • Facility security plan (A) • Access control and validation procedures (A) • Maintenance records (A) 	<p>Global DataGuard’s Network Access Control and Monitoring capabilities will help you to define secure boundaries to manage and monitor access to information and applications across multiple systems and disciplines. Our security products can easily and intelligently define who can access information, from which locations, and at what times. With Global DataGuard, you can efficiently and cost-effectively set the right balance between secure access for authorized users and highly secure boundaries that prevent unapproved access or intrusion.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Log Management & Monitoring • Network Access Control & Monitoring • Professional Services
<p>Workstation Use 164.310 (b)</p>	<p>This standard states that covered entities must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.</p> <p>A workstation is defined as an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, including electronic media stored in its immediate environment.</p> <p>There are no additional implementation specifications in the Workstation Use standard.</p>	<p>Global DataGuard’s Professional Services team will work with you to establish and test policies and procedures to ensure that workstation environments are logically partitioned into appropriate network security zones so that only approved information can be accessed by approved users from a specific location.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Professional Services



Standard	Summary of Requirements	Solutions
Workstation Security 164.310 (c)	<p>This standard states that covered entities must implement physical safeguards for all workstations that access EPHI in order to restrict access to authorized users only.</p> <p>There are no additional implementation specifications in the Workstation Security standard.</p>	<p>Global DataGuard provides you with immediate single-source access to all threat data, including an easy-to-use, instant view of prioritized security threats and the underlying data that created them.</p> <p>Our security dashboard enables you to instantly identify the most critical network threats, determine the best path for remediation and gather data for forensic reporting.</p> <p>And our vulnerability scanner provides customizable, on-demand scanning so that you can run scans, view alerts and run detailed reports with recommended actions in real-time.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Vulnerability Management• Threat Management• Professional Services
Device and Media Controls 164.310 (d) (1)	<p>This standard states that covered entities must 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 the facility.</p> <p>There are four implementation specifications in the Device and Media Controls standard. These include:</p> <ul style="list-style-type: none">• Disposal (R)• Media re-use (R)• Accountability (A)• Data backup and storage (A)	<p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Professional Services

TECHNICAL SAFEGUARDS

Standard	Summary of Requirements	Solutions
<p>Access Control 164.312 (a) (1)</p>	<p><i>R = Required; A = Addressable</i></p> <p>This standard states that covered entities must implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.</p> <p>Access control is defined as the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.</p> <p>There are four implementation specifications in the Access Control standard. These include:</p> <ul style="list-style-type: none"> • Unique user ID (R) • Emergency access procedure (R) • Automatic logoff (A) • Encryption and decryption (A) 	<p>From network access control and monitoring to threat and log management/monitoring, Global DataGuard has the full suite of enterprise-class tools and services to help you easily demonstrate compliance with HIPAA requirements.</p> <p>Our product portfolio, combined with world-class professional services, allows you to track individual users regardless of their IP addresses; handles security and access for remote and mobile workers; and provides a clear path to enhanced compliance and auditing requirements.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Log Management & Monitoring • Network Access Control & Monitoring • Data Leakage Monitoring • Data Encryption & Monitoring • Threat Management™ • Professional Services
<p>Audit Controls 164.312 (b)</p>	<p>This standard states that covered entities must implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.</p> <p>There are no additional implementation specifications in the Audit Controls standard.</p>	<p>Global DataGuard’s Professional Services team can help you evaluate and implement audit control plan, as well as make actionable recommendations for areas in need of improvement in relation to HIPAA requirements.</p> <p>Additionally, our team of experts will regularly audit policies to ensure ongoing alignment with HIPAA requirements, perform on-going rule-set changes and monitor these devices for any signs of attack.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Network Access Monitoring • Log Management, Monitoring & Retention • Vulnerability Management • Threat Management™ • Professional Services



Standard	Summary of Requirements	Solutions
Integrity 164.312 (c) (1)	<p>This standard states that covered entities must implement policies and procedures to protect EPHI from improper alteration or destruction. Integrity is defined as ensuring that data or information has not been altered or destroyed in an unauthorized manner.</p> <p>There is one implementation specification in the Workstation Use standard. It includes:</p> <ul style="list-style-type: none">• Mechanisms to authenticate electronic protected health information (A)	<p>Global DataGuard's Professional Services team can help implement policies and procedures to protect EPHI from improper alteration or destruction, as well as make actionable recommendations for areas in need of improvement in relation to HIPAA requirements.</p> <p>Additionally, our team of experts will regularly audit policies to ensure ongoing alignment with HIPAA requirements, perform on-going rule-set changes and monitor these devices for EPHI compliance violations.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Network Access Monitoring• EPHI Data Leakage Monitoring• EPHI Data Encryption & Monitoring• EPHI Log Management, Monitoring & Retention• Professional Services
Person or Entity Authentication 164.312 (d)	<p>This standard states that covered entities must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.</p> <p>There are no additional implementation specifications in the Person or Entity Authentication standard.</p>	<p>Global DataGuard's Professional Services team can help implement policies and to procedures to verify that a person or entity seeking access to EPHI is the one claimed, as well as make actionable recommendations for areas in need of improvement in relation to HIPAA requirements.</p> <p>Additionally, our team of experts will regularly audit policies to ensure ongoing alignment with HIPAA requirements, perform on-going rule-set changes and monitor these devices for EPHI compliance violations.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none">• Network Access Monitoring• EPHI Data Leakage Monitoring• EPHI Data Encryption & Monitoring• EPHI Log Management, Monitoring & Retention• Professional Services

Standard	Summary of Requirements	Solutions
<p>Transmission Security 164.312 (e) (1)</p>	<p>This standard states that covered entities must implement technical security mechanisms to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.</p> <p>There are two implementation specifications in the Transmission Security standard. These include:</p> <ul style="list-style-type: none"> • Integrity controls (A) • Encryption (A) <p>The appropriate control should be determined through a risk analysis to ensure that EPHI is protected in a manner commensurate with the associated risk when it is transmitted from one place to another. With regard to unsolicited EPHI –e.g., in email from patients—protection must subsequently be afforded once that information is in the possession of the covered entity.</p>	<p>Global DataGuard’s Firewall Management Solution, which utilizes Virtual StrongBox™ technology, can securely monitor and analyze encrypted data files without ever having to decrypt the data. This integrated managed firewall solution can capture, monitor and store log files from a variety of third-party firewalls, switches, routers, and applications running on servers. Further, it addresses data storage, local encryption, and key management requirements and provides comprehensive file-level security by incorporating the following unique and trusted technologies: Autonomous File-Level Security, Key Management, Identity Management, and Policy Management.</p> <p>Global DataGuard’s multi-layered security software includes Zero-Hour Virus Protection that proactively identifies outbreaks as soon as they emerge; RPD-Enabled Anti-Spam that detects and blocks spam automatically and remains consistently effective in the face of repeated and evolving spammer attempts; and IP Reputation service that fights spam and email-borne malware at the perimeter, reducing up to 90% of incoming messages at the entry-point, before they enter the network.</p> <p>How does Global DataGuard help?</p> <ul style="list-style-type: none"> • Firewall Management & Monitoring & VPN • Email Encryption • Network Access Monitoring • Professional Services

ADDITIONAL RESOURCES

HHS Office for Civil Rights HIPAA Information page <http://www.hhs.gov/ocr/hipaa/>

CMS HIPAA Regulations and Guidance page <http://www.cms.hhs.gov/home/regsguidance.asp>

Security Solutions for Healthcare <http://www.globaldataguard.com/solutions/hipaa.php>

ABOUT GLOBAL DATAGUARD

Based in Dallas, Texas, Global DataGuard is the premier provider of Enterprise UTM solutions for small/medium businesses to large enterprise organizations. Global DataGuard’s intelligent, out-of-the-box and fully integrated Enterprise UTM security suite has the necessary tools to arm first responders with preemptive, actionable remediation data to meet their unique compliance needs. Products and services include firewall, antivirus/anti-spam protection, IP Reputation, a web content filter, intrusion detection and prevention, adaptive network behavior analysis and correlation, network access and policy management, vulnerability management, threat management, and log management and monitoring.



2009 Best Products & Services – Reader’s Trust Award
Network Products Guide has named Global DataGuard a winner of the 2009 Best Products and Services - Reader’s Trust Award for Unified Security.



2009 'Tomorrow's Technology Today' Award
Info Security Products Guide has named Global DataGuard’s Enterprise UTM++ a winner of the 2009 Tomorrow’s Technology Today Award for the Integrated Security Solution (Hardware and Software) category. Global DataGuard has also received the Tomorrow’s Technology Today award in prior years (2006, 2007 & 2008) for Unified Security, Network Security and Security Risk Management Managed Security Services.



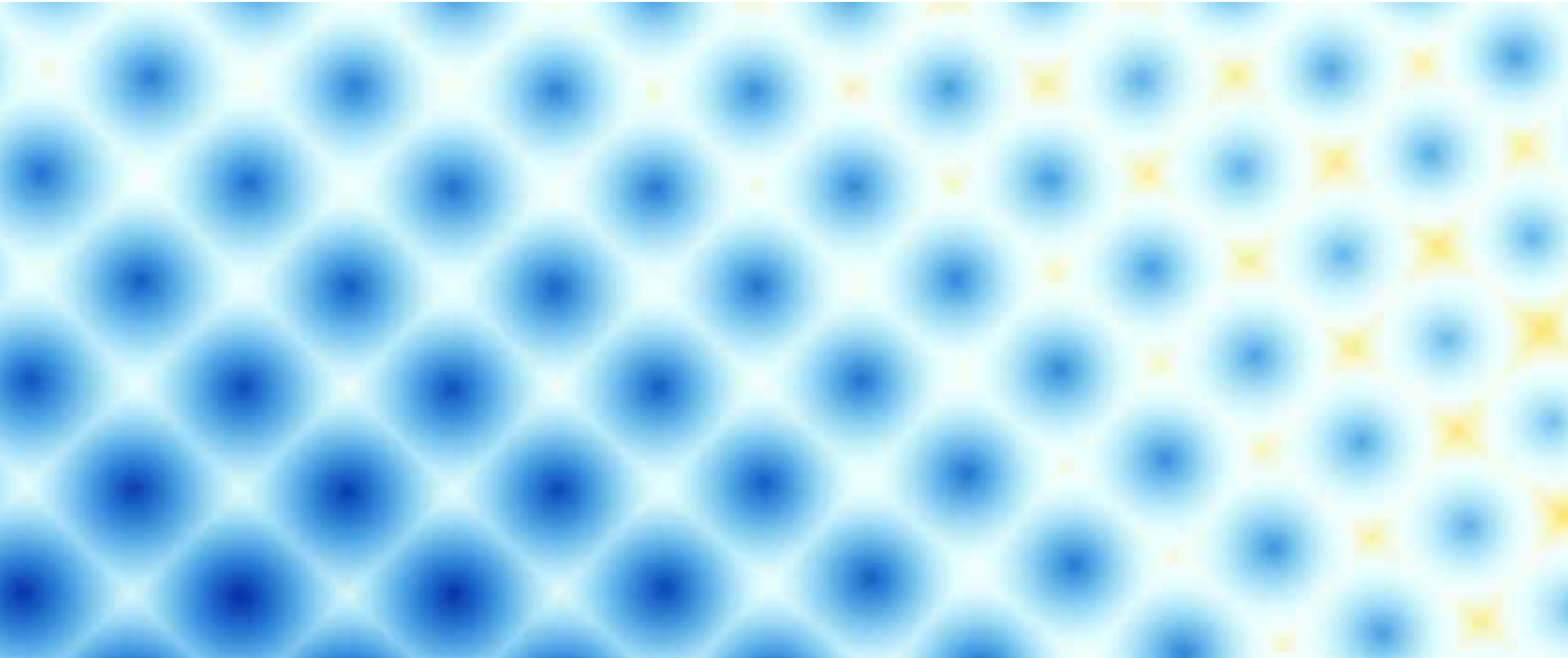
2009 Global Product Excellence - Customer Trust Award
Info Security Products Guide has named Global DataGuard a winner of the 2009 Global Product Excellence Customer Trust Award for Integrated Security.



SC Magazine 2008 Industry Innovator
SC Magazine has recognized Global DataGuard for its industry innovation in the unified threat management category.



2009 Product Innovation Award
Network Products Guide has named Global DataGuard’s Enterprise UTM++ a winner of the 2009 Product Innovation Award for the overall Security Solution (Hardware and Software) category. Global DataGuard also receive the Product Innovation award in 2008 for its All-n-One Security Module for Enterprise UTM.



14800 Landmark Blvd, Suite 610 | Dallas, TX 75254 |
972.980.1444 | www.globaldataguard.com



Global DataGuard