message archive search message archive search message archive search

Compliance Solutions

FOR HEALTH CARE

- HEALTH CARE PROVIDERS
- HEALTH PLANS
- HEALTH CARE CLEARINGHOUSES
- BUSINESS ASSOCIATES

HIPAA & HITECH Requirements and Global Relay Solutions for Electronic Communications Recordkeeping & Supervision

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Health Information Technology for Economic & Clinical Health Act (HITECH)

WELCOME AND THANK YOU for your interest in Global Relay's messaging compliance services for HIPAA regulated organizations. We are confident that you will find that our compliance solutions exceed your expectations.

COMPLIANCE is more than just the preservation of records to ensure that your organization can survive regulatory, audit and evidentiary scrutiny. It's a matter of Reputation, Integrity and Control. The stakes are high and they are tied to the prosperity of your organization. The compliance burden should no longer be thought of as solely a back office or IT matter. It should involve pro-active decision-making on the part of senior management to choose a high quality compliance solution to efficiently retain, protect, manage and ensure authenticity of records and to implement safeguards and internal supervisory controls against inadequate data management practices. Selecting a message archiving solution should be thought of as an investment in your organization's future, both in terms of risk reduction and overall firm image.

GLOBAL RELAY'S TECHNOLOGY SOLUTIONS reflect "best practices" standards that have become the benchmark for message management and compliance. Global Relay Archive and Compliance Reviewer are specifically engineered to provide a total regulatory and legal compliance solution for organizations subject to the regulatory compliance requirements of the HIPAA & HITECH Acts. Our services provide reliable, cost-effective and scalable message management and compliance solutions that:

- are seamlessly implemented within hours, with no software or hardware requirements or other capital outlays
- are continuously and seamlessly updated to meet current technological, legal and regulatory needs
- provide end-user tools, including mobile apps for iPhone, iPad, Blackberry and Android

KNOW YOUR VENDOR. As the developer, owner and operator of our technology, we have provided message archiving solutions since 1999 without a single incident of data loss. Each year, we engage KPMG to perform independent testing and validation upon our business, operational and security controls and report upon findings. KPMG also conducts independent security penetration testing procedures on our Internet-facing systems and applications. This comprehensive third party validation, available upon request, is unique in the hosted messaging industry.

Further, our health care compliance solutions are more than best-of-breed technology. We are a dedicated team of professionals with the highest synergy of business, technical and legal expertise. With 24x7x365 IT support, full-time in-house compliance lawyers, and professional Audit & eDiscovery and Data Services teams, we help our customers on a daily basis troubleshoot and resolve key IT and business issues, as well as play a mission critical role in your equation to achieving corporate excellence. We will provide your organization with a superior balance of technology, service, support, training and affordability to efficiently assist you in meeting regulatory, audit, corporate governance, discovery requests and other business needs.

YOUR COMPLIANCE SOLUTION will be tailored, without extra cost, to fit the needs of your organization, whether it is an independent business with outsourced email or a single server environment, or a multinational enterprise with disparate email and messaging systems (i.e. multiple servers/multiple platforms).

Call Global Relay at +1.866.484.6630 or visit us at www.globalrelay.com, and let us demonstrate how our best- of-class solutions will make the difference in winning you as a customer.

Yours truly,

Shannon Rogers
President & General Counsel

TABLE OF CONTENTS

Global Relay Archive

Assisting HIPAA Regulated Organizations in Meeting their Electronic Recordkeeping and Data Protection Requirements

For more information

Please refer to the following Global Relay publications:

- Global Relay Services Guide: a complete overview of all Global Relay compliance, message archiving, support, and professional services.
- Global Relay Compliance Solutions Guidebooks: additional publications detailing how Global Relay addresses the message archiving and compliance needs of:
  - Broker-Dealers (FINRA & SEC)
  - SEC Regulated Firms (Investment Advisors, Hedge Funds & Private Equity)
  - CFTC Regulated Firms
  - FCA (UK) Regulated Firms
  - Canadian Financial Firms (IIROC & MFDA)
  - Public Companies (Sarbanes-Oxley)
  - Enterprises

Available upon request

- KPMG Report on Global Relay's Business, Operational and Security Controls: provides assurances and transparency into the high standards of Global Relay's internal controls, and how these truly differentiate Global Relay
- SOC audit reports on Global Relay's two mirrored east/west coast data centers

Also refer to the following HIPAA documents, which can be found online:

- Department of Health and Human Services, Administrative Data Standards and Related Requirements, Security and Privacy Regulations (45 CFR Part 164): http://www.ecfr.gov/cgi-bin/text-idx?SID=c9a252f652b9e8aecc0f3d8fbfc032ee&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
- Health Information Technology for Economic and Clinical Health Act (Title XIII of the American Reinvestment and Recovery Act of 2009): http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf
- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

SERVICES

At-A-Glance

Global Relay Archive

Securely captures and preserves email, instant messaging, mobile messaging, social media, and more. Check with Global Relay if you need to archive a message type that is not listed here.

Compliance Reviewer

Complete message supervisory system that is configured to enforce and monitor your supervisory policies and procedures.

Audit and eDiscovery

Solutions are readily accessible within Global Relay Archive, providing efficient online tools for collaboration, case management and responses to legal data requests.

Global Relay Search

Provides users with 24/7 "anywhere access" to archived data via Blackberry, iPhone, iPad, Android, Outlook and the Web.

Global Relay Message

Global Relay's flagship messaging and unified collaboration communications service, designed to address the messaging, federation, compliance, privacy and security needs of firms in regulated industries. Global Relay Message is currently in beta.

Global Relay services are presented in three "pillars":

message

- **Global Relay Message**[1]
  Secure, fully compliant messaging platform
- **Email Services**
  Secure email with spam and virus filtering, shared calendars and contacts
- **Message Hub**
  Federate your Microsoft OCS/Lync with Thomson Reuters Messaging

archive

In-house, Hosted Exchange, Zimbra, Notes, Google Apps and more

BlackBerry, aim, THOMSON REUTERS, ice, BLOOMBERG®, pivot, slack, chatter, yammer, Instagram, YouTube, jive, Cisco Jabber, G+, LinkedIn, twitter, web, facebook, Lync

search

- Access messages anytime, anywhere
- Search across all message types
- Easily Reply, Reply All, Forward and Recover messages
- SAML enabled

1. Global Relay Message is our messaging and collaboration platform. In Beta - available soon.

The HIPAA and HITECH Acts

Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in response to dramatic advances in technology. HIPAA established security standards to safeguard protected health information created, transmitted or stored electronically (ePHI). The Act also restricts the use and disclosure of PHI in any medium (electronic, paper, or oral) to protect patient privacy. HIPAA requires "covered entities" (health care providers, health plans, and health care clearinghouses) and their business associates to:

- implement privacy and security policies
- train their workforce in these policies
- reasonably mitigate data leak risks and address security breaches in a timely fashion
- implement administrative, physical, and technical data safeguards
- put procedures in place for individual patients to register complaints

Health Information Technology for Economic and Clinical Health Act (HITECH)

In 2009, Congress passed the Health Information Technology Act (HITECH) as part of the American Recovery and Reinvestment Act. The Act required modifications to HIPAA rules to enhance patient privacy, increase patients' rights to access their PHI, expand the definition of business associates, and toughen enforcement of health care privacy laws. The modified rules became effective on March 26, 2013. The modifications include:

- Business Associates - The definition of a business associate has been expanded and clarified to cover all organizations that create, receive, maintain, or transmit PHI on behalf of a covered entity. The definition now explicitly includes patient safety organizations, health information exchange organizations, e-prescribing gateways, regional health information organizations, and organizations that provide data transmission services unless they only access data on a "random or infrequent basis." This "conduit" exception is narrow and is only intended to exclude organizations acting solely as "courier services." An organization that stores or maintains protected health information on behalf of a covered entity is a business associate regardless of whether it views the information it holds. Business associates must comply with the Security Rule and certain provisions of the Privacy Rule.
- Third Party Disclosures - HITECH places additional restrictions on disclosures of PHI for marketing and fundraising, and prohibits the sale of PHI without individual authorization. It also requires modifications to covered entities' notices of privacy practices.
- Breach Notifications - Covered entities are required to notify affected individuals and the Department of Health & Human Services (HHS) of a PHI breach. Business associates are required to inform covered entities of breaches. Any data breaches affecting over 500 individuals must be posted on the HHS website.
- Enforcement - HITECH strengthens the government's ability to enforce health care privacy laws by increasing civil suit penalties and establishing more objective standards of non-compliance.

In this Publication

This booklet describes how Global Relay can assist organizations in meeting HIPAA and HITECH requirements by adopting appropriate privacy and security controls for electronic communications.

REQUIREMENTS AND BENEFITS

Message Archiving

Global Relay helps HIPAA regulated organizations stay organized, compliant, and in control of their electronic communications. By implementing Global Relay Archive, covered entities and business associates can meet HIPAA and HITECH requirements, protect themselves against possible litigation, alleviate their IT burden, and increase employee productivity.

	Challenges	Global Relay Solution
Medical Record Retention	Patients increasingly expect to communicate with their health care providers electronically – by email or even text message. Providers may also communicate with each other electronically. Electronic messages containing information related to a patient and his or her health care, or used to make a decision related to patient care, may be part of the patient's medical record and therefore subject to retention requirements. HIPAA regulations mandate a 6 year retention term for certain types of records, including documentation of patient complaints and privacy notices, as well as records which fall under the "designated record set" to which covered entities must provide patients with access when requested. State regulations mandate minimum medical record retention periods ranging from 5-10 years after date of discharge or last date of services.	◦ Ensure medical records are complete and accurate to support the highest level of care. ◦ Automatically capture and preserve a complete set of all incoming, outgoing and internal emails and other electronic communications. ◦ Store multiple tamperproof copies of electronic communications in two mirrored east/west coast SOC audited data centers. ◦ Secure ePHI contained in electronic communications with dual encryption at rest. ◦ Set retention policies to ensure compliance with regulatory requirements. ◦ Ensure the confidentiality, integrity, and availability of ePHI contained in electronic communications.
Litigation and Malpractice Suits	Health care providers and related organizations face significant business and legal risks related to medical malpractice and other litigation, claims, and liability. They may also be subject to regulatory audits that can result in large fines for any identified violations. Electronic communications can supply valuable evidence in these cases to prove "who said what when" – provided organizations can locate these communications and produce evidentiary quality copies. Conversely, organizations may be unable to defend themselves if critical records are no longer available.	◦ Proactive protection and reduced eDiscovery costs. ◦ Authentic, evidentiary quality records for court. ◦ 24x7x365 online retrieval of any electronic communication within seconds. ◦ Quickly locate relevant messages amid large volumes of data via intuitive and advanced search tools. ◦ Filter, cull, and classify data; manage eDiscovery workflows through case management tools. ◦ Online production of data for external counsel or auditor review. ◦ Production of data in a standards-based format (e.g. PST) for court – within 24 hours.

	Challenges	Global Relay Solution
Risk Management	Organizations are liable for all messages distributed through their corporate systems (including personal communications). Mismanaging critical information puts an organization's professional reputation in jeopardy and undermines stakeholder confidence. Whether employees are communicating with co-workers, patients, or business associates, electronic messages are essential business communication tools that should be managed as an integral part of an organization's risk management program.	◦ Indisputable, chronological, time-date stamped records help safeguard organizations in the event of patient, business associate, or employee issues, errors or allegations. ◦ Establish supervisory controls to enforce message usage policies, reduce legal risks, and improve employee awareness of potential legal exposure. ◦ Implement customized rules to flag and review messages that may violate corporate policies or regulatory requirements.
Message Management	Ever increasing volumes of electronic communications put a heavy burden on IT staff to prevent data loss. Backups are widely used to protect critical data, but are difficult to manage and require huge amounts of expense and time to recover data when it is needed. For employees, mailbox size often does not keep pace with the growing number of messages they send and receive every day. They may delete messages that contain critical information or organize and retain their messages locally and idiosyncratically - making it difficult to locate and review messages across the organization.	◦ Reduce storage and backup time on live messaging systems ◦ Configure smaller email mailboxes ◦ Provide all employees with a "personal archive" of their own historical messages ◦ Maximize employee productivity with 24x7x365 online access to their messages via web, Outlook, and mobile devices ◦ One click recovery of deleted messages to Outlook

Benefits of the Cloud

- Focus on core business. Organizations can take advantage of the full redundancy, massive scalability and multi-layered security of Global Relay's systems while focusing their own resources on their core businesses - not on IT.
- Predictable and affordable costs. Global Relay provides services for a predictable monthly user fee. There are no large up front capital outlays, maintenance costs, or upgrade costs.
- Full support. Services are fully and professionally managed by Global Relay, with 24x7x365 live technical support, as well as training, legal, audit, and eDiscovery support, included at no additional cost.
- High Performance Technology. Global Relay Archive is a proprietary solution designed in-house by a team of 160+ developers and engineered for security, scalability, and high availability.

Security Rule

Significance of Rules

The Security Rule sets national standards for the security of electronic protected health information (ePHI). It requires all covered entities and business associates to establish and maintain rigorous security controls to ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit. Security standards are organized into three categories: administrative safeguards, physical safeguards and technical safeguards. To ensure organization-wide compliance with these standards, regulated organizations should identify all sources and locations of ePHI (including electronic communications), assess the associated security risks, and implement appropriate controls to mitigate these risks.

Who Must Comply

Health care providers, health plans, health care clearinghouses, and business associates who create, receive, maintain or transmit ePHI must comply with the Security Rule.

Requirements

In connection with the Security Rule, organizations must:

- ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit
- develop and implement security measures that allow them to reasonably and appropriately meet security standards and specifications
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI
- protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under HIPAA regulations
- implement policies and procedures to address security incidents
- implement administrative safeguards to prevent, detect, contain, and correct security violations
- implement physical safeguards to restrict access to information systems and facilities containing ePHI
- implement technical safeguards to prevent unauthorized access to ePHI

Repercussions of Non-Compliance

The Department of Health and Human Services, Office for Civil Rights has the authority to administer and enforce HIPAA regulations and has investigated claims against hospital chains, group health plans, national pharmacy chains, major medical centers, and small provider offices. A civil money penalty may be imposed if HHS determines that a violation has occurred. For violations occurring after February 18, 2009, HHS may impose penalties based on four levels of violations, with corresponding increases in fines. These penalties range from $100 to $1,500,000 for each violation.

Global Relay's Solution

Confidentiality, integrity and availability are the fundamental drivers behind all of Global Relay's services. To ensure the secure and accurate collection, processing and storage of customer data, as well as to prevent unauthorized access, modification or disclosure of data, industry best practices are deployed at every step. Because any security is only as strong as its weakest link, Global Relay arms itself with only the best: two world-class SOC audited data centers (including a private facility owned and operated by Global Relay), a high performance systems infrastructure, 24x7x365 system monitoring by senior system administrators, highly redundant archive systems, military-grade encryption, and experienced, well-trained employees.

Privacy Rule

Significance of Rules

Covered entities and business associates are responsible for complying with increasingly complex, comprehensive regulations to safeguard patient information. The Privacy Rule prohibits covered entities and business associates from using or disclosing PHI except as permitted or required by HIPAA regulations. The Privacy Rule applies to the use and disclosure of all PHI held or transmitted by an organization in any form or media – electronic, paper, or oral. Due to the growth of email, IM, text messaging, and other electronic message types as principle business communication tools in the health care industry, controls designed to protect against unlawful use and disclosures of information via electronic communications should be a fundamental part of a HIPAA regulated organization's privacy policies and procedures.

Who Must Comply

Health care providers, health plans, health care clearinghouses, and business associates who create, receive, maintain or transmit PHI must comply with the Privacy Rule.

Requirements

The Privacy Rule enumerates the permitted uses and disclosures of PHI by covered entities and business associates. The PHI that organizations have a responsibility to protect is broadly defined and includes: personal medical records, genetic information, conversations concerning patient care, billing transactions, and most personally identifiable health information. Permitted uses and disclosures include:

Covered Entities

- to the individual
- for their own treatment, payment, or health care operations
- to another covered entity for treatment, health care operations or payment activities
- to business associates if satisfactory assurance is obtained that the associates will safeguard the information as required by HIPAA regulations
- when required by HHS as part of an investigation into their compliance with HIPAA regulations
- in the course of a judicial or administrative proceeding
- as otherwise permitted by HIPAA regulations

Business Associates

- as permitted by their business associate contracts
- as required by law
- when required by HHS as part of an investigation into their compliance with HIPAA regulations
- to covered entities, individuals, or individuals' designees to satisfy an individual's request for a copy of PHI
- as otherwise permitted by HIPAA regulations

Global Relay's Solution

Global Relay Archive provides administrative tools that allow HIPAA regulated organizations to easily store and retrieve electronic communications while still restricting use and disclosure in compliance with the Privacy Rule. Archived data is secured through administrative, physical and technical safeguards as required by the Security Rule while remaining available online 24x7x365 for authorized users. Organizations can granularly control access to their archived electronic communications, ensuring users only have the minimum necessary privileges to meet patient care and organizational objectives.

Security Rule (45 CFR 164.3)

The Security Rule requires covered entities and business associates to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. Global Relay meets these standards and their implementation specifications as follows:

Administrative Safeguards			
§164.308	Standard	Global Relay's Compliance Solutions	
Security Management Process (a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Protecting Customer Data - Global Relay has implemented comprehensive security policies, procedures, and controls to protect customer data. These include a wide variety of measures, including ongoing risk analysis and management through: ◦ Automated and peer code review for all software releases as part of our formal software development lifecycle (SDLC) ◦ Strong network security, including firewalls and intrusion detection systems ◦ 24x7x365 monitoring of systems by Global Relay system administrators ◦ Daily vulnerability scans and annual penetration testing ◦ Regular review of system and security logs ◦ Disciplinary procedures for non-compliance with security policies (including possible termination of employment) Customer Tools – Global Relay Archive provides detailed logging of activity that can be reviewed by authorized customer personnel, including: ◦ Audit Trail - An unalterable audit trail appended to each archived message that logs any action taken against a message, (e.g. when it was imported, the retention term set, by whom it was viewed and when, etc.). ◦ Event Log - Documents user access (including logins, logouts and timeouts), added/modified/disabled users, changes to access rights, and more.	
	Implementation Specifications		
	Risk Analysis (a)(1)(ii)(A)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	✓
	Risk Management (a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	✓
	Sanction Policy (a)(1)(ii)(C)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	✓
	Information System Activity Review (a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	✓

Administrative Safeguards cont'd			
Assigned Security Responsibility (a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Global Relay's Information Security organization is led by an Information Security Manager who works with key personnel from teams across the organization to manage technology risks.	
Workforce Security (a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Customer administrators control all access to archived data by their own employees via Global Relay Archive's intuitive online administrative tools. Access can be granted, modified, and/or removed online 24x7x365. Examples include: Personal Archives - Employees can have access to their own historical messages via web browser, Outlook, and mobile apps. eDiscovery – Internal or external legal counsel can be given access to data relevant to a specific matter or litigation. This access can be as broad or as narrow as required (e.g. access only to the messages of custodians involved in the litigation). **Note**: Global Relay captures, preserves, and provides secure access (for authorized customer users) to an organization's electronic communications. Global Relay personnel do not read or use archived data. Access to customer data is restricted to a small number of senior personnel on an "as needed" basis in order to perform their duties (e.g. system support). Upon termination physical and logical access to Global Relay systems and facilities is rvoked immediately.	
	Implementation Specifications		
	Authorization and/or Supervision (a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	✓
	Workforce Clearance Procedure (a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate	✓
	Termination Procedures (a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	✓
Information Access Management (a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	See §164.308 (a)(3)(i)	
	Implementation Specifications		
	Access Authorization (a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	✓
	Access Establishment and Modification (a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	✓

Administrative Safeguards cont'd			
Security Awareness and Training (a)(5)(i)	Implement a security awareness and training program for all members of its workforce (including management).	Security Training and Awareness - All new Global Relay hires complete an on-boarding process that includes a security seminar led by Global Relay's Information Security Manager. This training is refreshed each year during an annual month-long security awareness campaign. In the interim, ongoing security awareness education seminars are conducted from both Security and Legal confidentiality/ privacy perspectives and the Information Security Manager regularly updates employees on internal and external security issues/events as they occur. Log-in Monitoring – Customer administrators can monitor log-ins to Global Relay Archive via an online Event Log (see §164.308 (a)(1)(i) for details). Password Management - Global Relay can authenticate against an organization's Active Directory/LDAP or integrate with Identity Providers (IdPs) that support SAML 2.0 (including ADFS). This allows customers to leverage their own password policies within Global Relay Archive and ensures Global Relay does not store or otherwise have access to passwords.	
	Implementation Specifications		
	Security Reminders (a)(5)(ii)(A)	Periodic security updates.	✓
	Protection from Malicious Software (a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.	✓
	Log-In Monitoring (a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.	✓
	Password Management (a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.	✓
Security Incident Procedures (a)(6)(i)	Implement policies and procedures to address security incidents.	Global Relay has an Information System Incident Response Team (ISIRT) led by the Information Security Manager and documented security incident handling procedures/policies.	
	Implementation Specifications		
	Response And Reporting (a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	✓
Contingency Plan (a)(7)(i)	Establish (and implement as needed) 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 electronic protected health information.	Global Relay's systems operate out of two mirrored east/west coast SOC audited data centers. The system is fully redundant within each data center and can take failures on every component without interruption. All archived data is replicated in near real time between Global Relay's mirrored data centers such that there are multiple copies preserved in geographically dispersed locations. In the event the primary data center is lost, the flow of data fails over to the secondary data center. Individual components of the service can also be failed over to the secondary data center.	
	Implementation Specifications		
	Data Backup Plan (a)(7)(ii)(B)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	✓
	Disaster Recovery Plan (a)(7)(ii)(A)	Establish (and implement as needed) procedures to restore any loss of data.	✓

Administrative Safeguards cont'd			
	Emergency Mode Operation Plan (a)(7)(ii)(C)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	✓
	Testing And Revision Procedures (a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.	✓
	Applications And Data Criticality Analysis (a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	✓
Evaluation (a)(8)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Global Relay annually engages KPMG to perform independent testing and validation on its business, operational and security controls and report upon findings. KPMG also conducts independent security penetration testing procedures on Global Relay's Internet-facing systems and applications. Specifically, the KPMG report provides customers with assurances of and transparency into Global Relay's internal controls related to: ◦ Physical Security - Safeguards governing data protection and data center controls. ◦ Change Management - Frameworks for guiding software development releases, operations and change control. ◦ Network Security & Availability - System architecture, redundancy, access and security. ◦ Message Processing - Inbound message processing, secure storage, data center replication and end-user access. ◦ Data Import, Extraction & Destruction - Policies, procedures and methodologies for securely handling customer data. ◦ Security Policies & Standards - Policies & standards governing privacy and confidentiality. ◦ Personnel Policies & Procedures - Employee life-cycle management. ◦ SAML Based Authentication - Verification of the security and correctness of the SAML authentication service.	
Business Associate Contracts And Other Arrangements (b)(1)	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Global Relay understands that performing due diligence on business associates is a responsibility and best practice for regulated organizations. Accordingly, Global Relay has contracted with KPMG for annual validation of its Business, Operational and Security Controls (see §164.308 (a)(8) for details). As well, Global Relay's two mirrored data centers undergo regular SOC audits. Additional documentation and assurances can be provided as part of customer due diligence.	
Subcontractors (b)(2)	A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	Global Relay understands that performing due diligence on business associates is a responsibility and best practice for regulated organizations. Accordingly, Global Relay has contracted with KPMG for annual validation of its Business, Operational and Security Controls (see §164.308 (a)(8) for details). As well, Global Relay's two mirrored data centers undergo regular SOC audits. Additional documentation and assurances can be provided as part of customer due diligence.	

Administrative Safeguards cont'd			
Written Contract or Other Arrangement (b)(3)	Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	Global Relay's in-house Legal team will prepare the required business associate contract using the business associate provisions provided by HHS.	
Physical Safeguards			
§164.310	Standard	Global Relay's Compliance Solutions	
Facility Access Controls (a)(1)	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.	Physical access to Global Relay's two mirrored data centers is strictly controlled through: ◦ 24 x7x365 uniformed guard service; ◦ Electronic access at entrances; ◦ Access limited to senior authorized Global Relay employees whose duties require access; ◦ Recording of date and timestamp each time a person enters and leaves either data center; ◦ Escort of all approved visitors by authorized Global Relay personnel ◦ Monitored CCTV camera surveillance and state-of-the-art alarm systems installed throughout the data centers	
	Implementation Specifications		
	Contingency Operations (a)(2)(i)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	✓
	Facility Security Plan (a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	✓
	Access Control And Validation Procedures (a)(2)(iii)	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.	✓
	Maintenance Records (a)(2)(iv)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	✓
Workstation Use (b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	As explained in §164.310(a)(3)(i), access to customer data is restricted to a small number of senior personnel on an "as needed" basis in order to perform their duties (e.g. system support). These personnel work out of Global Relay's secure data centers (see §164.310 (a)(1) for details) and headquarters. Global Relay's headquarters is secured with an electronic access control system on all doors, monitored alarms, and a gated reception area.	
Workstation Security (c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	See §164.310 (b)	

Physical Safeguards cont'd			
Device and Media Controls (d)(1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Change Management - All system changes and maintenance, including software and hardware changes are approved by Global Relay's Data Centre Management team or Change Management group, as appropriate. Data and Media Disposal - Deletion of archived data must be authorized in writing by the customer's authorized signatory or Appointed Administrator. Organizations can implement a "Rolling Deletion" policy to auto-purge message whose retention term has expired. All storage media are forensically wiped using a standard that exceeds the DOD standard, degaussed, and rendered unusable prior to physical destruction. Data Backup – All archived data is replicated in near real time between Global Relay's two mirrored data centers such that there are multiple copies preserved in geographically dispersed locations.	
	Implementation Specifications		
	Disposal (d)(1)(i)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	✓
	Media Re-Use (d)(1)(ii)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	✓
	Accountability (d)(1)(iii)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	✓
	Data Backup and Storage (d)(1)(iv)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	✓
Technical Safeguards			
§164.312	Standard	Global Relay's Compliance Solutions	
Access Control (a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	User Access Management - Authorized customer administrators have absolute granularity in all system administrative controls, including customizable Access Control Lists (ACL) to manage and enforce all user permissions. ACL's can be modified online 24x7x365 Unique User Identification – All customer users have unique user IDs to access Global Relay Archive. Automatic Logoff – Customer administrators can configure automatic timeout values for Global Relay Archive user sessions. Once a session has timed out, the user must re-authenticate to gain access to Global Relay Archive.	
	Unique User Identification (a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	✓
	Emergency Access Procedure (a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	✓
	Automatic Logoff (a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	✓
	Encryption and Decryption (a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	✓

Technical Safeguards			
Audit Controls (b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	See §164.308 (a)(1)(i).	
Integrity (c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Global Relay Archive preserves quality, accurate and complete records. Global Relay's internal business, operational, and security controls, including the message processing procedures, are annually validated by KPMG. The KPMG Report can be provided upon request. Quality - Global Relay Archive only imports data that meets quality standards. Failed messages (i.e. messages unable to be properly processed and indexed) are placed in a 'Not-Processed' bin as a result of malformed headers or corruption. Global Relay system administrators monitor these bins regularly and will either fix the issue or advise the Support team, who can engage with the customer in order to resolve. Accuracy - All messages are preserved on tamperproof storage with write-verification. There is no opportunity for users to modify or delete messages within the user interface (UI). Completeness - All messages are captured automatically, with no user intervention. Daily archiving reports are sent to customer administrator(s) to verify all data is properly archived.	
	Implementation Specifications		
	Mechanism To Authenticate Electronic Protected Health Information (c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	✓
Person or Entity Authentication (d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Only authenticated users can access Global Relay Archive. Global Relay Archive natively enforces username and password authentication over HTTPS. Alternatively, customers can authenticate against their AD/LDAP or SAML Identity Providers (IdPs).	
Transmission Security (e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	All data in transit in secured via TLS. See §164.312(a)(1) for details on encryption of data at rest.	
	Implementation Specifications		
	Integrity Controls (e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	✓
	Encryption (e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	✓