EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

Achieving HIPAA Compliance with The Evolve IP Compliance Cloud™

This white paper outlines how the security safeguards of *The Compliance Cloud*™ (Evolve IP's virtual private cloud) effectively and efficiently address the HIPAA requirements in regards to the privacy and security of electronic protected health information.

Overview

As innovation and regulation drive rapid evolution in the healthcare space, security and flexibility with mandated healthcare-related compliance are top of mind for healthcare leaders. These same drivers are providing opportunities and, in some cases, consternation for IT professionals and compliance officers. Specifically, healthcare providers must ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA), which requires entities to comply with specific security, privacy and breach notification rules for the storage and transmission of protected health information (PHI) including electronic data. These rules were further strengthened by the Health Information Technology for Economic and Clinical Health (HITECH) Act and most recently, redefined by the Omnibus Rule to include such entities as IT service providers.

Customers and providers share the commitment of hosting an application in compliance with HIPAA-HITECH rules. For cloud providers, there is not an official "HIPAA certification" or "HIPAA certified hosting" designation that can be achieved. However, for security decision-makers and administrators who are looking for best-in-class approaches for meeting regulatory compliance, *The Evolve IP Compliance Cloud*™ delivers all the controls and security safeguards needed to meet, and in many instances exceed HIPAA requirements for cloud providers. In addition to the HIPAA-HITECH compliant offering, Evolve IP is amongst the few managed cloud services providers that signs HIPAA Business Associate Agreements (BAAs) with customers, demonstrating our commitment to the proper storage and security of ePHI.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – The Basics

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA", 45 CFR Part 160 and subparts A and C of Part 164) was designed to promote the confidentiality and portability of patient records, as well as to develop standards for consistency in the health care industry. The Act has two (2) main rules: Privacy and Security.

The Security Rule (45 C.F.R. §164.306)[1] establishes a national set of minimum security standards for protecting all ePHI that a covered entity (CE) and business associate (BA) create, receive, maintain, or transmit. The Security Rule contains the administrative, physical, and technical safeguards that CEs and BAs must put in place to protect the confidentiality, integrity and availability of ePHI.

The following types of electronic data are examples of PHI covered under the Security Rule:

- Patient billing and administrative information exchanged with payers and health plans.
- Utilization and case management data, including authorizations and referrals that are exchanged with payers, hospitals and utilization management organizations.
- Patient health information gathered from or displayed on a Website or portal.
- Lab and other clinical data electronically sent to and received from outside labs.
- Word-processing files used in transcription and other kinds of patient reports that are transferred electronically.
- E-mails and voicemails between physicians and patients, and between attending and referring physicians and their offices.

In 2003 the Health Information Technology for Economic and Clinical Health Act ("HITECH", 74 Fed. Reg. 42740) expanded many of the requirements contained in HIPAA. The most notable HITECH provisions centered on notification requirements for ePHI breaches and stiffer penalties for non-reporting.

In 2013 the HIPAA Omnibus Rule (78 Fed. Reg. 5566) made significant changes in the HIPAA privacy, security, breach notification and enforcement rules, and expanded the definition of business associate (BA) to include an entity that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity. BA's must enter into a Business Associate Agreement (BAA) with their subcontractors. Any organization that touches ePHI needs to have a BAA in place.

Who Must Comply with HIPAA Regulations?

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, healthcare clearinghouses, and certain healthcare providers.

Covered entities include:

- Healthcare providers (engaged in services as a provider of medical or other health services, and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business).
- Health plans (individual or group plans that provide, or pay the cost of, medical care).
- Healthcare clearinghouses (public or private entities that provide billing services, re-pricing companies, community health management information systems, etc.).

Covered entities often use the services of a variety of other persons or businesses to conduct aspects of their healthcare related activities and services. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Business associates include:

- Entities that provide services to a covered entity that involve access by the business associate to ePHI and,
- Entities that create, receive, maintain, or transmit ePHI on behalf of another business associate.

The Omnibus Rule makes it very clear that cloud providers are considered business associates, stating: "document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold." As a BA, cloud providers must establish appropriate measures that address the physical, technical and administrative components of patient data privacy and security.

While the Security Rule does not apply to patients, once electronic data is received by a covered entity, it becomes protected by the HIPAA Rules[2].

For tools and resources to support your Health IT Privacy and Security initiatives, visit:
https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

Implications and Opportunities

Healthcare providers can better control their costs by moving their communications and cloud computing systems to the cloud. This takes away the burden and expense of managing on-premises equipment and provides access to the latest technological advancements. To maintain HIPAA compliance, cloud service providers must deliver secure and compliant solutions that continuously evolve and support changing regulatory requirements.

Covered entities (for example, Evolve IP healthcare customers) are ultimately responsible for the security of their HIPAA data, encrypting the sensitive data anywhere it is transmitted or stored, including in the cloud environment, since protecting the confidentiality, integrity, and availability of ePHI is the essence of the HIPAA Security Rule.

Because cloud providers typically store, transmit, or process ePHI, they must also comply with the HIPAA standards to meet HIPAA compliance. The same risk analysis, administrative, physical and technical safeguards, and ongoing due diligence apply just as much in the cloud provider's data center environment as in a covered entities' facility. Additionally, since cloud providers are considered business associates, they must have a BAA in place with the covered entity, as well as with any subcontractors (for example, backup vendors) that store, process or transmit ePHI of the covered entity or business associate.

Failure to comply with HIPAA requirements can lead to severe consequences. In addition to penalties and fines, non-compliant organizations face reputational damage, loss of business, and legal liability.

The Solution Provider Role and Accountability

Covered entities (for example, Evolve IP customers) are ultimately responsible for the security of their ePHI data, including encrypting the sensitive data anywhere it is transmitted or stored, including in the cloud environment.

As previously stated, there is no "HIPAA certification" or "HIPAA certified hosting" designation that can be achieved. What the cloud providers can help customers with is, to ensure that the services provided to them meet the requirements of cloud providers for the administrative, physical, and technical safeguards and standards set forth by the HIPAA, HITECH and Omnibus Acts.

Customers are responsible for configuring their applications, platforms, websites and portals in a HIPAA-compliant manner, for restricting and monitoring access to their ePHI data, and for enforcing policies in their organizations to meet HIPAA compliance.

What Makes Evolve IP "Best of Breed" for HIPAA Compliant Hosting?

The Evolve IP Compliance Cloud™ supports the regulations of HIPAA, HITECH and Omnibus Acts. Additionally, Evolve IP has the ability to sign HIPAA Business Associate Agreements (BAAs) with customers, demonstrating its commitment to the proper storing and security of ePHI on behalf of customers subject to HIPAA regulations.

For covered entities, *The Compliance Cloud*™ delivers the following:

Cloud Model

- Evolve IP uses a private cloud model for HIPAA customer environments. Each customer has a dedicated virtual switch that routes traffic through their own dedicated firewall; this design model provides complete segregation between customers.
- A third-party SOC 2 review of the Evolve IP cloud environment was performed by an Independent Service Auditing firm. This review culminated in a favorable report; a summary report of which is available to customers and potential customers.
- An independent third-party HIPAA Compliance review was performed of the Evolve IP cloud offering. This review culminated in a favorable report; a summary report of which is available to customers and potential customers.

Restricting Data to the USA

- Evolve IP uses GeoIP filtering for all HIPAA customer firewalls that restricts inbound and outbound communications to USA-based IP addresses.
- Evolve IP uses GeoIP filtering for all HIPAA customer outbound emails that restricts email to email domains that have USA-based IP addresses.
- Evolve IP uses primary and redundant data centers located only in the U.S. Cloud backup provider Intronis securely stores customer backup data in Eastern and Western U.S. facilities.

Restricting Access to Customer Data

- Evolve IP limits access to customer firewalls, routers, switches, and other infrastructure equipment to authorized Evolve IP administrators and engineers.
- Customers are responsible for creating their system administrators, individual users, and creating access to resources (fileservers, directories, etc.).
- Physical access to Evolve IP data centers requires two-factor authentication, and is restricted to approved Evolve IP personnel.

HIPAA Administrative Controls

- Evolve IP has implemented an annual risk assessment process that requires Information Owners to identify significant threats to security, availability, and confidentiality and to implement appropriate measures to monitor and manage these risks.
- Evolve IP's information security team monitors the system and assesses the system vulnerabilities; additionally, all IDS alarms are reviewed, escalated and corrective actions are implemented.
- Evolve IP has compliance, data backup, disaster recovery and incident management plans.

HIPAA Physical Controls

- Evolve IP requires that all visitors must sign in at the front desk and be escorted in all Evolve IP locations.
- Evolve IP securely removes all customer data from all devices upon termination of services.

- Evolve IP restricts movement within its facilities by use of access badge restrictions.

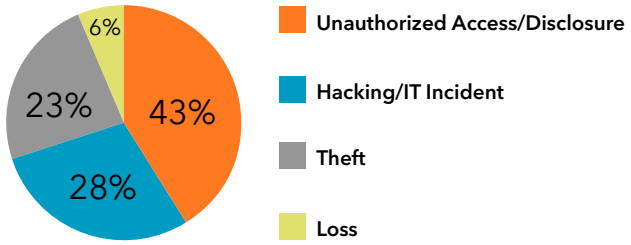
HIPAA Technical Controls

- Evolve IP uses logging to monitor customer logins to their servers and environment.
- Evolve IP provides Intrusion Prevention/Intrusion Detection Services (IPS/IDS) at the individual customer firewall edge of their network. All events and logs are continually streamed to a secure 24x7 event monitoring center.
- Evolve IP uses data storage in customer environments that employs a FIPS 140-2 level of certification for data at rest, and industry-accepted encryption methods for data in transit to and from the covered entities' locations to the Evolve IP locations (includes VPN tunnels and virtual desktop access).

Types of Breaches

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals.

Of the 91 incidents reported between January and April 2016, Unauthorized Access/Disclosure ranked as the most common type of breech.



Source: Office of Civil Rights (OCR) *https://ocrportal.hhs.gov*

Achieving HIPAA Compliance With Evolve IP

Essential to any compliance program is the establishment of responsibilities and accountabilities addressing both the solution provider and the customer. The following Shared Security Responsibility matrix identifies HIPAA controls and the assignment of responsibility and accountability between Evolve IP (cloud provider) and the customer (covered entity):

Control	HIPAA Control Specification	Evolve IP	Customer
A1	Risk analysis (Required)		✓
A2	Risk management (Required)	✓	✓
A3	Sanction policy (Required)		✓
A4	Information system activity review (Required)	✓	✓
A5	Identify the security official who is responsible for the development and implementation of the policies and procedures.		✓
A6	Authorization and/or supervision (Addressable)	✓	✓
A7	Workforce clearance procedure (Addressable)		✓
A8	Termination procedures (Addressable)		✓

Control	HIPAA Control Specification	Evolve IP	Customer
A9	Isolating health care clearinghouse functions (Required)		✓
A10	Access authorization (Addressable)	✓	✓
A11	Access establishment and modification (Addressable)	✓	✓
A12	Security reminders (Addressable)	✓	✓
A13	Protection from malicious software (Addressable)	✓	
A14	Log-in monitoring (Addressable)	✓	✓
A15	Password management (Addressable)	✓	✓
A16	Response and Reporting (Required)	✓	✓
A17	Data backup plan (Required)	✓	✓
A18	Disaster recovery plan (Required)	✓	✓
A19	Emergency mode operation plan (Required)	✓	✓
A20	Testing and revision procedures (Addressable)	✓	✓
A21	Applications and data criticality analysis (Addressable)		✓
A22	Evaluation		✓
A23	Written contract or other arrangement (Required)	✓	✓
P1	Contingency operations (Addressable)	✓	✓
P2	Facility security plan (Addressable)	✓	
P3	Access control and validation procedures (Addressable)	✓	
P4	Maintenance records (Addressable)	✓	

Control	HIPAA Control Specification	Evolve IP	Customer
P5	Workstation use		✓
P6	Workstation security	✓	✓
P7	Disposal (Required)	✓	
P8	Media re-use (Required)	✓	
P9	Accountability (Addressable)	✓	
P10	Data backup and storage (Addressable)	✓	
T1	Unique user identification (Required)	✓	✓
T2	Emergency access procedure (Required)	✓	✓
T3	Automatic logoff (Addressable).	✓	
T4	Encryption and decryption (Addressable).	✓	✓
T5	Audit controls.	✓	✓
T6	Mechanism to authenticate electronic protected health information (Addressable).		✓
T7	Standard: Person or entity authentication.	✓	✓
T8	Integrity controls (Addressable).		✓
T9	Encryption (Addressable).	✓	✓
O1	Business associate contracts (Required).	✓	✓
O2	Standard: Requirements for group health plans. (Required).		✓
D1	Standard: Documentation.	✓	✓

Product Guidance

Evolve IP offers various products to suit a wide range of customer needs. When purchasing cloud services for your compliance project, please specify with your Evolve IP Technology Advisor, that you are seeking the added value and security available exclusively with *The Evolve IP Compliance Cloud*™.

Your Technology Advisor can assist you with a menu of Evolve IP Compliant SKU's for Communications, Desktops, Email, Servers, Storage and Backup to ensure you are selecting *The Compliance Cloud*™.

Conclusion

While there are complex variables relating to HIPAA, Evolve IP delivers the technology and expertise to help customers confidently meet compliance requirements for hosting their EPHI data. Designed to deliver data-centric security architecture, military-grade encryption, and robust auditing features, *The Compliance Cloud*™ provides security decision-makers and administrators with a virtual private cloud that meets, and in many instances exceeds HIPAA requirements.

Learn More

For more information on *The Evolve IP Compliance Cloud*™ including additional security and compliance offerings, visit:
http://www.evolveip.net/solutions/compliance.encryption

References

1. *The Security Rule*
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

2. *Guide to Privacy and Security of Electronic Health Information*
https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

About Evolve IP

The Cloud is no longer about buying individual services. It's now about building a strategy around multiple cloud services and integrating them together to make IT more efficient. Evolve IP delivers customized strategies and integrated services for both cloud computing and communications; solutions that are designed to work together, with your current infrastructure, and with the applications you already use in your business. Disaster Recovery, Contact Center, Unified Communications, Desktops and Infrastructure … Experience Cloud as a Strategy™