Barracuda

Solution Brief

HIPAA Compliance with Barracuda Archiving

The healthcare industry relies on data to provide effective patient care. This sensitive data must be easily accessible by healthcare providers, while kept safe from inappropriate parties and accidental loss.

Patient medical records and other personal information are increasingly transmitted electronically by email, and the Health Insurance Portability and Accountability Act ("HIPAA") sets forth the standards for protecting this data.

Barracuda Message Archiver and the Barracuda Cloud Archiving Service provide secure archive storage for email data. They manage end user access to this data and can support a healthcare institution's compliance activities, thereby assisting it with meeting HIPAA requirements.

What is HIPAA Compliance?

HIPPA is the primary United States law governing the protection of patient health information. Signed into law in 1996, HIPAA has since been supplemented and clarified by the Health Information Technology for Economic and Clinical Health (HITECH) Act and various health and Human Services (HHS) regulations, including the 2013 Omnibus Rule.

Originally, HIPAA's requirements were targeted at Covered Entities—health plans, healthcare clearinghouses, and healthcare providers that transmit any health information electronically. However, many of the law's provisions, including the Security Rule, apply equally to Business Associates of healthcare organizations. More specifically, Business Associates are organizations that create, receive, maintain, or transmit PHI on behalf of Covered Entities. As such, providers of IT services must secure any PHI held in the cloud on behalf of Covered Entities and provide functionality to ensure the confidentiality of PHI in the cloud.

The HIPAA regulations set forth various data privacy and security provisions that aim to safeguard health-related information. HIPAA is designed to protect personally identifiable patient information and prevent it from being accessible to the general public. The two areas within HIPAA that are covered by this solution brief are the **Security Rule** and the **Privacy Rule**.

HIPAA Security Rule

The HIPAA Security Rule requires organizations to safeguard all Protected Health Information ("PHI") that it creates, receives, maintains or transmits in electronic form, including email. Under the Security Rule, organizations subject to HIPAA are required to maintain reasonable and appropriate administrative, technical, and physical safeguards to protect this data.

The Security Rule is flexible and scalable to allow organizations to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate will depend on the nature of the business as well as its size and resources.

HIPAA Privacy Rule

The HIPAA Privacy Rule regulates whether and how organizations may use or disclose PHI. An organization may not use or disclose PHI in any way except in the very specific circumstances defined in the rule. For example, the Privacy Rule allows organizations to use or disclose PHI for the purposes of treatment, payment, or healthcare operations. It can also be disclosed to the individual who is the subject of the information.

Is Archiving Essential for Compliance?

HIPAA requires that organizations keep PHI secure for an extended period of time in order to demonstrate compliance and to respond to information requests. This includes, for example, maintaining a record of all email containing PHI. Archiving email is an easy and effective way to ensure compliance with HIPAA.

Barracuda's email archiving solutions provide customers with infrastructure and processes that can assist an organization with meeting the technical, administrative and physical safeguards specified in the HIPAA Security Rule. Built-in access and audit controls will enable an organization to safeguard the integrity of PHI and prevent its improper modification or deletion.

Barracuda's email archiving solutions also assist organizations with HIPAA Privacy Rule compliance. Authorized individuals can search and retrieve historical email as necessary in order to extract data about a patient, support litigation or eDiscovery exercises, and respond to audit requests from the Department of Health and Human Services.

How Barracuda Archiving Supports Compliance

The Barracuda Message Archiver and Barracuda Cloud Archiving Service support compliance with HIPAA in the following key areas:

Accurately Capture Data

Organizations must retain an accurate copy of all electronic communications containing PHI.

- The Barracuda Message Archiver and Barracuda Cloud Archiving Service use SMTP Journal Capture to secure a copy of each email "in motion" at the time it is sent or received. This approach ensures that an accurate and unmodified copy of every email sent or received, including details of all recipients, will be captured without an opportunity for amendment or deletion.

Keep Data Secure

Organizations must ensure PHI data is protected from being amended, corrupted, or destroyed.

- Barracuda stores a single immutable copy of every email outside the production email environment in a separate secure archive repository, either in a dedicated hardware, virtual appliance, or in Barracuda's Cloud.
- The Barracuda Message Archiver is typically deployed behind an organization's firewall and is protected by the same security used to protect primary data sources. Data replicated to the Barracuda Cloud is encrypted for transmission and storage using a 256-bit AES algorithm.
- Data transmitted to the Barracuda Cloud Archiving Service using SMTP can be protected with TLS encryption, and all data stored in the Barracuda Cloud Archiving Service is also encrypted with a 256-bit AES algorithm and remains encrypted until requested for retrieval.

Keep Data for as Long as Required

Electronic communications containing PHI must be retained for a minimum of six years.

- Barracuda provides retention policies that—when configured properly—can retain data for a specified period of time and be deleted when no longer needed.
- These policies are highly configurable and cover a broad range of criteria, such as message type, content, source, addresses, age, and attachments.

Produce Data When Needed

Organizations must be able to search and retrieve emails as necessary in order to extract data about an individual, support litigation, or comply with an audit request from the Department of Health and Human Services.

- Barracuda employs an indexing process that catalogs all email content, including metadata and attachments. This feature is complemented with searching capabilities that have an intuitive user interface enabling end users to undertake their own search and retrieval activities without involving IT staff.
- Subsets of data can be tagged for further analysis or for inclusion in subsequent iterative search activities. Finally, selected data can be exported as needed for subsequent analysis or production to third parties.

Manage Access to Data

HIPAA requires that system access controls are implemented to safeguard the integrity of PHI data and to govern which users are able to access this data.

- Barracuda provides role based access controls that operate at the individual user level to ensure that only authorized users are able to access archived data. These controls can also be configured to determine the exact scope of data records that each individual user is allowed to access.
- IP login restrictions can be set for administrative users of the Barracuda Message Archiver and to prevent access from IP addresses outside a specified range.

Provide System Audit Controls

Organizations must maintain an accurate record of all activities relating to their stored PHI data, including details of every access made to that information.

- Barracuda's archiving solutions maintain a complete audit trail of every activity by administrators and end users, including the date, time and IP address for each user login, plus a full audit trail of all system activities.
- The audit trail also details each time a record is stored, retrieved or exported, so Barracuda can provide a full chain of custody for all archived data.

Business Associate Agreements (BAA)

Organizations storing PHI in offsite locations must comply with sections 164.314, 164.502 and 164.504 of HIPAA, which require Covered Entities to sign Business Associate Agreement ("BAA") with their Business Associates. A BAA is a legal agreement in which a Business Associate makes various commitments regarding the security and privacy of PHI held on behalf of the Covered Entity.

Barracuda may be considered a Business Associate of a Covered Entity customers that use Barracuda's Cloud Archiving Service and for customers that use Cloud Storage with their Barracuda Message Archiver. To the extent Barracuda is a Business Associate under the HIPAA regulations, Barracuda complies with any applicable HIPAA requirements.

Customers wishing to establish a Business Associate relationship with Barracuda for the purposes of compliance with HIPAA should request a Business Associate Agreement from Barracuda.

If a customer is a Business Associate of a different organization that is a Covered Entity, and the customer stores PHI in the Barracuda cloud, then under HIPAA Barracuda is a subcontractor to the customer. In such instances, when requesting a copy of Barracuda's standard Business Associate Agreement, the customer must specifically request the version that reflects Barracuda's status as a subcontractor of the customer.

Barracuda's standard Business Associate Agreement has been updated in response to the 2013 Final Rule.

Conclusion

HIPAA regulations require that healthcare organizations develop and follow strict procedures to ensure the confidentiality and security of PHI whenever it is transferred, received, handled, or shared.

The Barracuda Message Archiver and the Barracuda Cloud Archiving Service can help organizations meet HIPAA requirements by capturing an accurate record of every email sent or received, storing this data securely and providing system controls to ensure that only authorized users have access.

Search and retrieval capabilities are provided to end users. Together with a comprehensive audit log of all activities, these features can enable organizations to undertake discovery activities needed to maintain HIPAA compliance.