druva

White Paper

Endpoint Backup Compliance Considerations for HIPAA-Regulated Enterprises

A guide for IT professionals in healthcare, pharma, and other regulated industries

Executive Summary

Information is the most valuable asset businesses have today; keeping it secure is a critical challenge for organizations of all sizes. As a result of the HITECH Act and the strengthening of privacy protections as required by the omnibus final rule, regulated companies and their business associates are now held to an even higher standard of information security. Organizations regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must shoulder the increasingly complex responsibility of ensuring that there is sufficient protection applied to all processes, devices and business associates that hold or have access to Protected Health Information (PHI). In an era of greater digital mobility, IT professionals need even tighter controls over administrative, physical and technical safeguards.

When speaking of the omnibus final rule, former U.S. Department of Health and Human Services (HHS) Secretary Kathleen Sebelius acknowledged the importance of safeguarding PHI in "an ever expanding digital age." In today's mobile workforce, 81% of employees access documents on the go[1] from an average of 3.3 connected devices.[2] Unfortunately, these devices and the data residing on them are often not adequately protected. According to the HHS, 750,000 individuals' PHI was breached in the first six months of 2014 because of theft, loss, or improper disposal of an endpoint device.[3] On top of being unable to safeguard sensitive data, highly regulated industries have much higher per capita data breach costs, with healthcare companies averaging 112% higher breach costs than the mean (Figure 1).[4] To best address HIPAA compliance in this mobile age and to maintain business productivity while actively mitigating risk, organizations need to respond to the challenge of protecting data and ensuring data privacy on all endpoint devices. Moreover, when considering deployment options, whether cloud or on-premise, enterprises need to ensure the same high standards for data security and privacy.

This white paper is meant for technology professionals tasked with the responsibility to protect sensitive data and PHI. The features and functions listed within have already been used by organizations to help comply with required and addressable specifications set forth in HIPAA/HITECH.

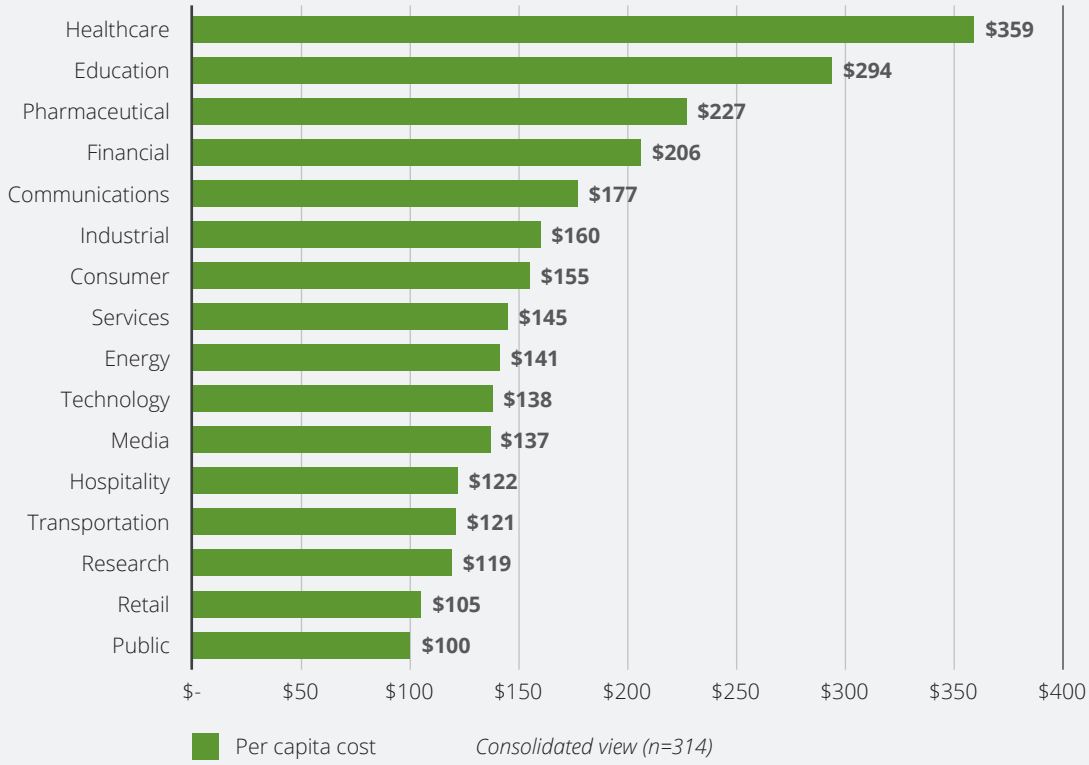
What HIPAA Means for Data on Endpoint Devices

To maintain confidentiality and integrity of Electronic Protected Health Information (EPHI) and to combat data breach risks, highly regulated organizations need an endpoint data protection solution with the right features to address administrative, physical, and technical safeguards as found in the Security Rule at 45 CFR §164.304. Such a comprehensive solution should protect against data loss and breach, ensure data privacy, and allow for data governance on endpoints so that only those with appropriate security clearance are able to access PHI.

The four HIPAA rules under discussion are the Security Rule, the Privacy Rule and the Enforcement and Breach Notification Rules.

1. Workshare
2. Cisco IBSG Horizons
3. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
4. Ponemon 2014 Cost of Data Breach Study: Global Analysis

Figure 1: Per Capita Cost by Industry Classification



More than 750,000 individuals' PHI was breached in the first six months of 2014.

HIPAA Security Rule

The Security Rule applies to PHI in electronic formats either transmitted by or maintained on electronic media. Covered entities that maintain or transmit protected health information are required by the Security Rule (see 45 CFR. §164.306) to:

- Ensure the confidentiality, integrity, and availability of all EPHI data
- Protect against any threats or hazards to the security or integrity of such information
- Protect against any uses or disclosures of such information that are not permitted
- Institute a contingency plan for an emergency that results in a major data loss

These requirements become harder to satisfy as users increasingly access EPHI on endpoint devices. Consider these startling numbers:

- 28% of corporate data resides exclusively on laptops and mobile devices;[5] but 35% of enterprise laptops are not backed up regularly.[6]

5. Gartner
6. ESG

28% of corporate data reside exclusively on laptops and mobile devices, but 35% of enterprise laptops are not backed up regularly.

- 76% of companies do not encrypt mobile devices,[7] 70% of corporate laptops are not encrypted and 90% of laptops do not have the ability to remotely wipe.[8]
- More than 50% of stolen laptops result in data breaches,[9] while 36% of data breaches are caused by inadvertent insider misuse.[10]

This means that if an endpoint device is lost, stolen or otherwise compromised advertently or inadvertently, a substantial amount of data will be rendered inaccessible, thus breaching the Security Rule.

Look for these features when you evaluate endpoint backup solutions:

- **Encryption: Data at rest**

  Cloud-based solutions should encrypt data at rest with both 256-bit AES U.S. government-standard encryption and a two-factor encryption mechanism. This ensures that no entity outside the customer (including the solution provider) has the ability to decrypt or gain access to PHI data without the knowledge or consent of the customer, effectively reducing the risk of unauthorized access.

  This approach is modeled after a bank safety deposit box, wherein the bank and the customer each retain separate keys and the box cannot be accessed with just one of the keys.[11]

- **Encryption: Data in transit**

  The solution should encrypt data with industry-standard 256-bit SSL secure communication protocol to ensure secure transmission. If the company is backing up its endpoints to the cloud, every client should securely authenticate with its solution provider before ever transmitting any data, including profile configurations. Having a secure channel ensures that all data is protected while in transit and will also reduce the risk of any person intercepting PHI data that may be transmitted over public networks.

- **Remote Wipe / Auto-Delete**

  The solution should have the ability to remotely and immediately decommission a device when potential PHI data is in jeopardy of unauthorized access. If a device is suspected of being compromised, a remote wipe command can be issued, immediately removing all protected information from the device. The solution should also allow a device to be automatically decommissioned and wiped if it does not "check in" with the solution system within a specific number of days, adding an extra layer of protection to the device when it's off-network.

- **Continuous Data Protection (CDP)**

  At a minimum, an endpoint data protection solution needs to allow an end user to create and maintain exact copies of EPHI and recover that data when a device is lost, stolen or simply malfunctions. Whether taking measures for a contingency plan or trying to enable better business functions, a reliable endpoint backup solution is essential. A risk management solution that offers automated and continuous data protection will enable more comprehensive recovery capabilities. Automation reduces human error such as forgetting to back up data and provides continuous data protection. This enables users to restore data to the most recent instance possible.

7. KRAA Security
8. Ponemon Institute
9. Grudi Associates
10. Forrester Research
11. Learn more in the Druva Security white paper; available upon request from Druva.

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information that applies to health plans, healthcare clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The rule requires appropriate privacy protection for personal health information and sets conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information, including rights to examine and obtain copies of their health records and to request corrections.

Business Associates are also directly liable for uses and disclosures of PHI that are not covered under their Business Associate Agreement (BAA) or the HIPAA Privacy Rule itself and the Privacy Rule requires Business Associates to do the following:

1. Prohibit impermissible uses or disclosures of PHI.
2. Provide breach notification to the Covered Entity.
3. Provide either the individual or the Covered Entity access to PHI.
4. Disclose PHI to the Secretary of HHS, if compelled to do so.
5. Provide an accounting of disclosures.
6. Comply with the requirements of the HIPAA Security Rule.

Because HIPAA-covered companies are held to an even higher standard of data privacy, they need a Business Associate with the solution that provides exceptional safeguards surrounding privacy and accessibility of PHI. While 45 CFR §164.304(b) gives companies the flexibility in choosing the type of technology used to enforce compliance, all endpoint solutions should have granular controls over data accessibility and provide complete data privacy and anonymity, no matter where the data resides.

The features to look for are:

- **Controlled access by authorized personnel only**
  The solution should have comprehensive and easily managed policy settings that only allow authorized users and designated admins with the right level of clearance to access the minimum data needed to perform job functions. Users should also be granted privacy controls that enable them to restrict access to their data - even by admins - as a higher level of PHI protection. As unauthorized access is a compliance violation under HIPAA, having multiple safeguards provides greater control and visibility into potential data risks, especially by allowing only authorized access and by providing full monitoring and reporting capabilities.

- **Integrated disablement of user access**
  The solution should be integrated with an identity provider system (SSO/SAML) and Microsoft's Active Directory so that when a user is removed or deactivated, the solution provider will reflect that change automatically. An integrated solution ensures that only authenticated entities can access or restore data; non-authenticated entities can be automatically blocked, thus reducing the risk of unauthorized access to PHI data.

- **Geofencing: Blocking access from unauthorized IP addresses**
  The solution should allow access levels to be determined by geographic IP ranges or by discrete domains to limit who can access the data solution system based on where that user is accessing data. Having the ability to control access via geographic IP and to block unauthorized domains provides organizations with full visibility into how data is accessed, and significantly mitigates the risk of unauthorized access to potential PHI data.

- **Authentication for data restore requests**

  The solution should offer both device-level authentication and another layer of authentication at the solution provider level when a user attempts to restore data. Having double authentication helps verify that the user requesting a data restore is authorized and has successfully authenticated their identity via their credentials. This reduces the risk of unauthorized persons gaining access to PHI data.

HIPAA Enforcement and Breach Notification Rules

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires entities and their business associates to provide notification following a breach of unsecured PHI. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, as well as financial penalties for violations of the HIPAA Administrative Simplification Rules and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

With strengthened enforcement standards post-HITECH, it's more critical now than ever for companies to provide accurate, timely notification upon potential breach and to aid in investigations. Otherwise, they risk hefty financial penalties and negative publicity. For example, a pharma researcher forgets her laptop on a train but is able to find it after two hours. Although the chances are that no one accessed the laptop during that time, the pharma company still needs to report, that for two hours, it didn't know the laptop's location or whether the data on it was secure. Even the mere possibility of a potential breach exposes an organization to negative publicity. This is why an endpoint data protection solution that is built with audit readiness in mind is essential for data governance.

These are the data governance features to look for in an endpoint backup solution:

- **Delegated administration**

  The solution should enable customers to have granular permission controls into access authorization by administrators, not just users. Only administrators with the proper authorization to work with such data should be granted access to administer users with the same authorization. This will reduce the risk of unauthorized persons gaining access to such data.

- **Geo-Location / Tracking**

  The solution should allow endpoint device tracking so that a device suspected of being lost or stolen can be identified and located, reducing the risk of misappropriation of PHI data. A device with tracking enabled is able to leverage a number of mechanisms, such as WiFi network names and IP addresses, to help identify its approximate location in the event of loss or theft.

- **Tamper-proof audit trails**

  The solution should record unalterable audit trails for both end users and administrators. Audit trails contain details that trace the history of the data. Having trace and audit trail search functionality enables organizations to better assess risk potential for data and to monitor and investigate suspicious system usage or access - necessary components for conducting and validating compliance programs.

Maintaining HIPAA-Compliance Regardless of Deployment

The solution provider needs to be HIPAA/HITECH compliant and ready to enter into a BAA on behalf of the customer. In addition, the solution should have the flexibility to implement on-premise or cloud deployments based on the customer's need and maintain appropriate safeguards whether data is stored on-premise or in the cloud. For solution providers backing up endpoint data to the cloud, the cloud infrastructure provider should meet high security standards, including redundant global data centers and industry-leading enterprise-level SLAs.

- **Partner with a business associate compliant with HIPAA/HITECH obligations**

  When choosing a vendor, it's also important for the solution provider to have passed independent review validating the company's security and privacy controls for handling PHI in a HIPAA-compliant manner. This way, the customer will be assured that the solutions provider will:

  - Not use or disclose PHI other than as permitted or required by the BAA or as required by law.
  - Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA.
  - Mitigate, to the extent practical, any harmful effect that is known to the vendor of a use or disclosure of PHI by the vendor in violation of the requirements of the BAA.
  - Report to the Covered Entity any use or disclosure of the PHI not provided for by the BAA of which it becomes aware.
  - Ensure that its agents, including subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to the BAA.
  - Make its internal practices, books, and records available to the HHS Secretary relating to the use and disclosure of PHI received from the Covered Entity for the determining of compliance with HIPAA for the Covered Entity.

- **Cloud deployment with a compliant service**

  For organizations interested in a cloud-based service, look for a provider with an audited environment that validates its security and privacy controls for handling PHI. This ensures all levels of the technology stack meet the guidelines required by HIPAA/HITECH. The cloud infrastructure should also be scalable, with multiple layers of operational and physical security.

  In addition, the cloud provider should have secure and extensively documented procedures to ensure adherence to industry best practices for operation and management of cloud computing solutions, such as SOC 1 (includes SAS-70 Type II, SSAE-16), and a backup vendor whose cloud operations are ISAE 3000 Type II-certified.

  This adherence should apply across all services offered by the solution provider to ensure customer data is never shared or accessible by another customer within the system.

- **On-premise deployment**

  Organizations that prefer not to utilize a cloud-based service should select a provider offering on-premise solutions, enabling organizations to leverage their own internal data centers for storage of PHI data.

Conclusion: HIPAA Compels IT Professionals to Scrutinize Endpoint Data Policies

Control over mobile devices is one of the weakest aspects of an organization's security management. While 75% of the workforce is now mobile,[12] only 19% of IT professionals know how much regulated data is on endpoint devices.[13] Data breaches cause financial, legal, business and reputational harm. With the average total organization cost of data breach being $5.9 million[14] and increased penalties for noncompliance under HIPAA, endpoint backup protection that mitigates data breach is necessary for modern regulated workforces. Fundamentally different from generic backup solutions, a comprehensive endpoint backup protection enables organizations to better address the high level of security needed when dealing with PHI on endpoint devices by protecting against data loss, ensuring data privacy, and establishing data governance on hard-to-track endpoint devices.

This document has outlined the primary components of what a data protection solution should have to assist entities that must comply with HIPAA regulations. The highlighted security features and safeguards will ensure that customer data is protected from access by the data solution provider or any other unauthorized persons. By understanding the critical function of these features and how they impact data security, an IT professional can make a more informed choice when evaluating a Business Associate partner in endpoint data protection.

Disclaimer: Druva can not itself guarantee an organization's compliance or that the information contained herein can affirm compliance for an organization. This duty is the responsibility of the customer to ensure that the controls listed herein meet the requirements as set forth in the HIPAA/HITECH Regulations, and as enforced by the U.S. Department of Health and Human Services. Please consult with your organization's legal department to identify if these controls are acceptable in meeting their interpretation of the sufficient means for your organization's compliance.

12. Forrester Research
13. Ponemon Institute
14. Ponemon 2014 Cost of Data Breach Study: Global Analysis

About Druva

Druva is the pioneer and market leader in data protection and governance at the edge of the enterprise, bringing visibility and control to business information in the era of the mobile workforce and consumerization of IT. Druva's solutions for managing data outside the corporate firewall reduce the loss of corporate information assets and address organizations' compliance, governance, forensics and eDiscovery needs. Headquartered in Silicon Valley with offices worldwide, Druva is privately held and is backed by Nexus Venture Partners, Sequoia Capital and Tenaya Capital. For more information, visit **www.druva.com** and connect at **www.druva.com/blog.**

More Resources

Learn more on how Druva helps healthcare and pharmaceutical companies with HIPAA compliance

For more resources, visit druva.com/resources.

More than 3,000 customers trust Druva for data protection including:

MERZ Pfizer Shire STERIS Hanger Empowering Human Potential

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com

0000-0000