



Microsoft SharePoint® for HIPAA/HITECH: Privacy Compliance Made Simple

Much of the coverage of The Health Insurance Portability and Accounting Act (HIPAA) has centered on the significant regulatory requirements it places on the healthcare industry. However, the Act is designed to safeguard Protected Health Information (PHI), while also allowing for the flow of electronic health information needed to provide and promote high-quality care.

Microsoft SharePoint is the ideal platform for health organizations who want to share information protected under HIPAA. The platform is easily designed and configured to help healthcare professionals streamline business operations, enhance collaboration among employees, and manage business-critical digital assets, while leveraging the tools they are already familiar with, including Microsoft Office and Outlook applications. SharePoint also supports Electronic Medical Records (EMR) initiatives by allowing content to be shared between facilities and providers, while medical researchers can use SharePoint as a platform for trend analysis on large amounts of disease-related data stored in Microsoft SQL server databases.

The benefits for healthcare organizations and, ultimately patients, that use SharePoint to better collaborate on and provide access to health information is clear; however making this information available without proper safeguards presents a serious risk of privacy breaches and HIPAA violations. HiSoftware Compliance Sheriff® for SharePoint® enables healthcare organizations to realize SharePoint's collaborative benefits while ensuring that PHI is not exposed to individuals who do not have a clinical requirement for access.

As detailed below, Compliance Sheriff for SharePoint can be easily applied to address the core compliance requirements of HIPAA. And because these privacy checkpoints are contained within our configurable rules engine, HiSoftware can also automate the enforcement of your organization's unique approach to HIPAA data compliance, wherever it may diverge from or extend beyond the standard requirements, taking into account your specific processes for data collection and storage, as well as your risk tolerance.

WHAT IS HIPAA?

As enforced by the Department of Health and Human Services' (HHS) Office of Civil Rights (OCR), HIPAA was the first federal attempt to address the privacy and security of health information in electronic form. As part of implementing HIPAA, HHS developed the HIPAA Privacy Rule, establishing national standards to protect individuals' medical records and other PHI. The Rule requires appropriate safeguards to protect the privacy of PHI, and sets limits and conditions on the uses and disclosures that may be made of such information without a patient's authorization.

The rule applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The HITECH Act, signed into law by President Obama in February of 2009, widens the scope of privacy and security protections available under HIPAA, increases covered entities potential legal liability for non-compliance and provides for more enforcement than HIPAA alone. For example, as mandated by the HITECH Act, the HHS has contracted with KPMG to conduct on-site HIPAA audits. Site visits conducted as part of every audit will include interviews with leadership (e.g., CIO, Privacy Officer, legal counsel,

health information management/medical records director) at the covered entity. The HITECH Act means that, depending on the severity of a breach or a HIPAA violation identified during an audit, organizations may be subject to fines and penalties in excess of millions of dollars.

HOW CAN HISOFTWARE HELP?

As part of enforcing HIPAA, HHS created the [Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information](#). In its Guidance on the Framework, HHS has identified eight key principles which, if followed, ensure compliance and encourage the electronic exchange of health information.

Openness and Transparency – *“There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information.”*

To ensure openness and transparency, every healthcare organization should have a privacy policy prominently displayed. Compliance Sheriff will scan all of your SharePoint properties to ensure that every page displays a functioning link to your privacy policy.

As mandated by the HITECH Act, HHS is now conducting on-site HIPAA audits. Is your organization ready?

Compliance Sheriff monitors your Web, extranet and intranet properties for Protected Health Information (PHI) including:

- Name & address
- Social Security number
- Medical record number
- Medical diagnoses
- Health plan beneficiary number
- Telephone number
- Email address
- Certificate/license number
- Internet Protocol (IP) address
- Finger or voice prints
- Photographic image



Collection, Use and Disclosure Limitation – *“Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.”*

Compliance Sheriff automatically scans both external and internally-available SharePoint sites, as well as any attached files, to detect the presence of PHI and instantly notify IT managers and/or relevant privacy managers of a potential breach. Depending on your organization's unique approach and policy requirements, you can use Compliance Sheriff to ensure that the methods used to collect PHI are secure, and that whenever that information is stored, accessed or moved, it is only by credentialed users and only to appropriate alternative locations.

Safeguards – *“Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.”*

Compliance Sheriff for SharePoint constantly scans data both at rest and in-motion to ensure that PHI is not being stored in areas where it can be accessed by non-credentialed users.

Compliance Sheriff can be used to provide notification of inappropriate disclosures of PHI, allowing organizations to provide prompt and time-sensitive notification that may prevent or limit the damage of a privacy breach.

Accountability – *“The Principles in the Privacy and Security Framework should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.”*

By providing multi-layered reporting, Compliance Sheriff for SharePoint delivers executive visibility into your HIPAA compliance status. All reports can be further drilled into to allow managers an opportunity to immediately remediate and report on any compliance issues or breaches.

Individual Choice Principle – *“Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.”*

As in the Openness and Transparency principle, Compliance Sheriff monitors relevant SharePoint sites to ensure that if a person is providing PHI in electronic form, they are able to easily review your privacy policy and opt-out of any disclosures or sharing of data before submitting the information.

Correction – *“Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.”*

Organizations can utilize Compliance Sheriff for SharePoint to proactively identify potential issues as well as ensure they have an accessible and protected manner for individuals to dispute the accuracy of their information via secure Web-enabled applications. This streamlines the efficiency and accuracy of the processes while building in compliance.

By combining monitoring and reporting capabilities with a set of configurable, HIPAA-specific rules, HiSoftware allows

your organization to document execution of your policy, ensure compliance with it and demonstrate to the OCR an ongoing effort to protect the personal health information you are currently managing in SharePoint.

Data Quality and Integrity – *“Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.”*

At the point of collection, Compliance Sheriff validates that information collected electronically is accurate. Fields can be examined to ensure required data is present and formatted properly. Data integrity is also a natural by-product of automated compliance monitoring, as you are more informed of what is happening with the health information you are managing.

Individual Access – *“Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.”*

Core to readability and availability of online medical records is the accessibility of that information to those with disabilities. Compliance Sheriff will ensure all your SharePoint sites (including the SharePoint framework itself) and the information displayed on them is accessible to all members of the public in accordance with Section 508 of The Rehabilitation Act and WCAG 2.0 standards.

FOR MORE INFORMATION

For more information on HiSoftware's automated SharePoint solutions for HIPAA data compliance, or to discuss your organization's specific system requirements, please call 1.888.272.2484 or email info@hisoftware.com to be connected with a solution specialist.



www.hisoftware.com

Corporate Headquarters

One Tara Boulevard, Suite 104
Nashua, NH 03062 USA
T: +888.272.2484 (U.S. & Canada)
+1.603.578.1870
F: +1.603.578.1876
E: info@hisoftware.com
 HiSoftware

EMEA

Hamilton House, Mabledon Place
Bloomsbury London WC1H 9BB UK
T: +44 (0) 207 953 0301
F: +1.603.578.1876
E: emea@hisoftware.com
 HiSoftware_EU