rubrik

Data Governance in Healthcare: Guide to HIPAA Compliance with Rubrik Polaris Sonar

Reduce Sensitive Data Exposure. Automate Consistent Processes with Policy-driven Simplicity.

The Health Insurance Portability and Accountability Act (HIPAA) is an evolving set of US Federal laws enacted to protect and secure electronic protected health information (ePHI) in order to ensure patient privacy and protect health information. Non-compliance can result in serious fines. In 2018, HIPAA enforcement set an all-time record with $28.7 million in penalties – a 22% increase from 2016[1]. Securing ePHI is a unique challenge since healthcare facilities are generally not highly secured data centers. They are by their nature physically open to visitors, distributed over locations (floors and wings), and some portions of the environment lack a traditional defensible perimeter. Adoption of cloud platforms and services can add further complexity. Rules are in place but mistakes happen.

THE ANATOMY OF HIPAA COMPLIANCE

Three important aspects of the combined regulation include:

The Privacy Rule - Requires that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.

The Security Rule - Operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (ePHI)

The Breach Notification Rule - Requires that affected individuals, the Health and Human Services Secretary, and in some circumstances, the media are notified within 60 days of a breach.

Source: hhs.gov website

Over the past 20 years new technologies have improved mobility, quality, and efficiency of the healthcare and insurance industries. Unfortunately with evolving technology comes complexity and with complexity also comes risk. An application could be writing to a poorly secured NAS share, or someone might have copied content "somewhere more accessible" and then forgot about it. Exposed data could also be discovered while conducting due diligence when integrating IT services post merger or acquisition.

Rubrik helps keep pace with these changes, and facilitates visibility into where sensitive ePHI is stored with automated data classification. Rubrik already protects the data, Polaris Sonar simplifies data compliance.

MEET POLARIS SONAR: AUTOMATED DATA GOVERNANCE TO ASSIST WITH HIPAA COMPLIANCE

Polaris Sonar is a SaaS application that uses machine learning to automatically discover and classify data.

To begin using Polaris Sonar for HIPAA automation, all a Rubrik customer has to do is turn it on and select a template. Polaris begins to scan the data in the background and flags data matching specific identifiers. Since production workloads are already being protected, the data to be analyzed exists within the Rubrik Cloud Data Management (CDM) repository. Sonar sweeps through protected environments searching for defined patterns whether the data is on-premises, in a remote office, or in the cloud. This means no agents to install, no heavy scans on production workloads, and most importantly no heavy lifting for the IT staff. Sonar delivers automation of policy management and very fast time to value, and it keeps running in the background without constant intervention, upgrades, or hardware refreshes.

[1] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html

USE CASES

FIND PATIENT DATA (ePHI)

Classify data
automatically

AUTOMATE SCANNING TO REDUCE RISK

Without impacting
production workloads

MAINTAIN AVAILABILITY

Instant recovery
Ransomware detection
Long-term low cost retention

Find Patient Data Stored in the Wrong Place

In general people don't try to expose healthcare records, but it can happen by accident. There is always the occasional situation where someone copies an entire folder or directory for easier access. Whether it is an authorized administrator that grants permissions too widely, a developer working with an improperly de-identified data set, or a well meaning staff member, ePHI may not be adequately protected. A simple wrong click or misconfiguration is all it takes and ePHI is exposed. The worst part is it can stay unnoticed for a long time.

Sonar scans data that has been protected by Rubrik to identify defined patterns. This can alert to exposed ePHI as part of an overall solution for risk analysis and mitigation. This, along with other organization-wide risk assessments, can collectively help to meet the requirement for organizations to analyze risk under 45 CFR 164.308(a)(1)(ii)(A) and 164.308(a)(1)(ii)(B).

Reduce ePHI Exposure Risk

Attackers looking for data to monetize will always go for the easy score. Vulnerable ePHI introduces a much higher risk of theft, where stolen records may be auctioned off to the highest bidder or leaked online. An embarrassing leak could become part of some extortion scheme, or the press could be alerted by some researcher who stumbles across it. Either way, disclosures could result in an audit, and an audit could turn up more exposed data. See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.404 and 164.408.

Sonar finds exposed ePHI automatically in the background, and finds it without having to go looking. Since the scans are continuously checking and analyzing protected data, quickly remediating exposure eliminates an attacker's low hanging fruit. Keeping data where it should be stored complicates the effort needed by an attacker to get to their goals, and the longer they dwell trying to get something, the more the chances are that they will be detected.

Keep ePHI Available with Rubrik

When a "security incident"[2] leads to unauthorized access, use, disclosure, modification, or destruction of ePHI, such as a ransomware attack, organizations must execute their security incident response procedures and, as needed, contingency plans.[3] Every minute that doctors and nurses don't have access to information needed to make clinical decisions.

The Polaris platform also provides a solution for detection and restoring data following a ransomware attack. Polaris detects anomalous behavior and provides a workflow recovery that takes the guesswork out of restoring data. An organization can use Polaris as part of their contingency plans (45 C.F.R. § 164.308(a)(7)) to instantly recover lost workloads and help an organization get back on its feet quickly.

Rubrik Protects Your Data

Patients have a right to their data, and if was accidentally deleted or not available for whatever reason then organizations face penalties. The Rubrik platform can help organizations meet their need to have accessible backups of ePHI in the event of an emergency. It can quickly and easily restore individual records or entire servers to meet the availability requirements. In addition, if records are misplaced then Polaris Sonar can perform a one time search and recover them even from unstructured stores.

[2] 45 C.F.R. §164.304
[3] 45 C.F.R. §164.308(a)(7)

According to HIPAA Journal OCR is cracking down on unavailability of records in 2019. "Denying patients copies of their health records, overcharging for copies, or failing to provide those records within 30 days is a violation of HIPAA."[4]

Reduce Disruption from Audits

Nothing invites an audit as quickly as a complaint about poorly secured data or a mandatory disclosure as a result of a breach. An audit as a result of a breach disclosure (or even a false alarm) introduces an unknown risk that something completely unrelated might be found. OCR auditors may very well clear the organization of any wrongdoing on the part of the breach, but then go on to find several previously unknown areas that do result in penalties. The risk from unknown threats is reduced with Polaris Sonar since it scans in the background and can find problem areas before they turn into trouble.

Rather than heavy lifting to create templates, with Polaris Sonar, your team has the tools to automatically check for policy compliance and remediate violations on a more regular basis without the intrusiveness of scanning production systems and without the need for indexing. Polaris Sonar includes pre-built templates to cover some of the typical use cases, but modifying or tuning a policy is flexible and intuitive. Either define a regex to match the patterns found in sensitive data, select a few words, or import an entire CSV dictionary. You can combine templates to create an overall policy that is just right for your organization.

Organizations must have the policies and procedures to protect the security and privacy of ePHI, however they also need to have the technical capability to support those policies. Polaris Sonar can be part of your toolkit to show auditors that you can identify where some types of sensitive data resides when managed by Rubrik CDM.

WHAT OUR CUSTOMERS ARE SAYING

City of Sioux Falls

"Data classification tasks that would have previously required expensive 3rd party auditors and multiple full-time engineers can now be completely automated. We drove over 90% operational savings by eliminating manual scripting and spreadsheet management, reducing time spent to complete hundreds of search queries from two weeks to just 1 hour," said Brandon Morris, Systems Administrator at City of Sioux Falls. "Not to mention, Sonar provides a platform to continuously monitor our sensitive data for high risk incidents, such as overexposed credit card numbers and social security numbers, seamlessly on our existing backup data without impacting production."

To learn more about Polaris Sonar and how it can help your organization automate their data governance requirements, please visit our website or contact your local sales person.

[4] https://www.hipaajournal.com/common-hipaa-violations/

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik, the Multi-Cloud Data Control™ Company, enables enterprises to maximize value from data that is increasingly fragmented across data centers and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility. For more information, visit www.rubrik.com and follow @rubrikInc on Twitter.