BigID

www.bigid.com • info@bigid.com • @bigidsecure

A Data Driven Approach for ePHI Protection

HIPAA Data Security & Privacy

Under the HIPAA mandate, covered entities and business associates are subject to the Security Rule that covers confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and the Privacy Rule that limits the uses and disclosures of PHI. These rules have long been in place, but how ePHI moves through and across IT infrastructure and is tied to Personal Information within IT systems and applications has shifted since the rules were first written. Also, the penalties levied by regulators for breach, unauthorized disclosure and privacy violations have escalated. BigID automatically discovers, maps and labels all instances of PHI identifiers and across data sources through novel correlation and machine learning technologies to drive both security and privacy compliance initiatives.

Assess ePHI Risk

HIPAA risk analysis and assessment has many components, but integral to making a informed risk analysis is a current and comprehensive understanding where ePHI is stored. Many healthcare organizations have clearly delineated and segmented operations, payments and transactions systems. However, once data moves out of these systems into unstructured data repositories through undocumented processes, such as patient identity saved to case management notes for example, organizations lose visibility and can no longer adequately assess risk. BigID's unique discovery and correlation capabilities automatically find all PHI in unstructured data stores - providing context that traditional pattern-matching approaches cannot. The technology utilizes enrichment techniques to associate data values with patient identities in structured datastores even if column, table and field names are inconsistent and cannot be captured through manual processes. Moreover, organizations can calibrate risk for individual data values by attribute, data source and application to inform how security measures are configured and to align with threat occurrence analysis.

ePHI Data Mapping

Mapping ePHI involves determining where that data is stored, what processing steps are involved and how the data flows internally and externally so as understand risks and the state of compliance. Building data maps based on stakeholder surveys can be laborious and manually intensive process with impressionistic, rather than accurate outcomes. Likewise, using tools that rely on Regular Expression pattern matching are prone to false positives, and cannot determine whether demographic identifiers should be classified as ePHI based on context, such as proximity to patient identifier. BigID automates the building and maintenance of data flow maps from actual system scan output across data sources with integrated ePHI classification. It also automates the ability to add context augmentation such as why ePHI is being collected or transferred for a specific processing step. As scans uncover new ePHI, or additional identifiers are classified as ePHI based on automated discovery, organizations can proactively identify compliance and initiate remediation steps like minimizing data.

BigID

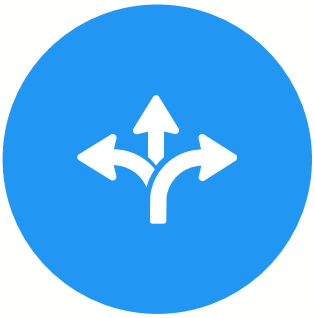
Your Customers' Privacy, **Protected!**

www.bigid.com • info@bigid.com • @bigidsecure

A Data Driven Approach for ePHI Protection

Breach Response

The HIPAA Breach Notification Rule requires covered entities and business associates to notify affected individuals, HHS and sometimes the media “without unreasonable delay” and no more than 60 days after a security breach is discovered if 500 or more individuals are affected. Many state laws require an even shorter notification timeline. Timely, effective and comprehensive breach response is contingent on whether organizations can expeditiously determine which identifiers, and whose data, were impacted. Based on BigID’s mapping and indexing of ePHI by data source, security teams can better understand their data breach risk and security measures applied. In the event of an incident or data breach, Security and IT teams can quickly scope the impact and understand which identifiers and attributes have been impacted by a breach based on BigID’s inventory of ePHI and identities by data source.



ePHI Classification and Labeling

While the HIPAA Security and Privacy rules define a specific set of identifiers under the PHI category, the rules apply to "individually identifiable information relating to the health status of an individual, the provision of healthcare, or individually identifiable information that is created, collected, or transmitted by a HIPAA- covered entity in relation to payment for healthcare services."
To comprehensively discover and classify ePHI across all data sources and determine whether an identifier relates to a specific individual in order to apply the appropriate security measures requires identity context. BigID utilizes correlation and machine learning to connect data elements back to the identity of the individual, improving the accuracy of determining what should be classified as ePHI. To simplify enforcement on classified data, BigID enables customers to automatically assign ePHI classification labels for files and tag data elements. These tags can be consumed by enforcement technologies such as Microsoft's Azure Information Protection or serve as input for de-identification processes.

How BigID Can Help

BigID is redefining personal data protection and privacy in the enterprise.
Organizations are facing record breaches of personal information and more onerous regulator enforcement and penalties - even as privacy expectations grow.
BigID gives organizations software to automate the security and management of structured and unstructured PHI data across datacenters and cloud. Using BigID, enterprises can better steward their most vital assets: their customer, employee and PHI data.
For more information, email info@bigid.com or schedule a demo at bigid.com/demo