

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect Personal Health Information (PHI).

Title II of HIPAA includes the Privacy Rule which regulates the use and disclosure of PHI held by health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers. HIPAA's Security and Privacy rules outline the requirements for Electronically Protected Health Information (EPHI). The Security Rule includes:

- Controlling and monitoring access to equipment containing health information.

5 Key Steps to Database Security Process Control

In order to effectively secure their databases, organizations must address five critical requirements:

1. **Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
2. **Eliminate Vulnerabilities:** Identify and fix vulnerabilities that are exposing the database on a continual basis.
3. **Enforce Least Privileges:** Reset user access controls and privileges to allow access to only the minimum data required for employees to do their jobs.
4. **Monitor for Deviations:** Implement appropriate policies and monitor for any and all activity that deviates from normal and authorized activity.
5. **Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

- Limiting access to hardware and software to properly authorized individuals.
- Protecting Information systems housing PHI from intrusion.
- Ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- Documenting risk analysis and risk management programs.

HIPAA is very specific in its requirements to protect any hardware or software containing Electronically Protected Health Information (EPHI) and draws upon the federal guidelines for security requirements.

NETWORK-CENTRIC VERSUS DATA-CENTRIC APPROACHES TO HIPAA

Many organizations start with a network-centric approach which focuses on the end points and periphery defense. Periphery defenses are limited in the protection they provide because:

- SQL injection vulnerabilities are prevalent and provide direct access to the database.
- Hackers are more successful loading malware onto employee workstations, providing a jump off point to the database and PHI.
- Insider attacks are on the rise.

It is therefore critical that organizations include a data-centric approach and protect the data where it lives – the database. Application Security's data-centric solution is Precision Database Activity Monitoring (DAM). Precision DAM enables organizations to secure their databases by controlling the security processes that impacts Personal Health Information.

FIVE STEPS TO COST-EFFECTIVE HIPAA COMPLIANCE

Step 1: Isolate Sensitive Databases

HIPAA requires healthcare organizations implement policies and procedures to prevent, detect, contain, and correct security violations. The first step to effective HIPAA compliance is to isolate all databases containing Personal Health Information. DbProtect's Database Discovery feature generates a complete inventory of all databases deployed enterprise-wide. It identifies all production, test, and temporary databases, and more importantly, any unauthorized databases. DbProtect's Sensitive Data Discovery identifies and locates all PHI residing on those databases. DbProtect helps organizations to protect their PHI by:

- Ensuring all PHI is located on authorized and secured databases.
- Restricting access and use of PHI.
- Identifying and removing any unauthorized databases from their networks.

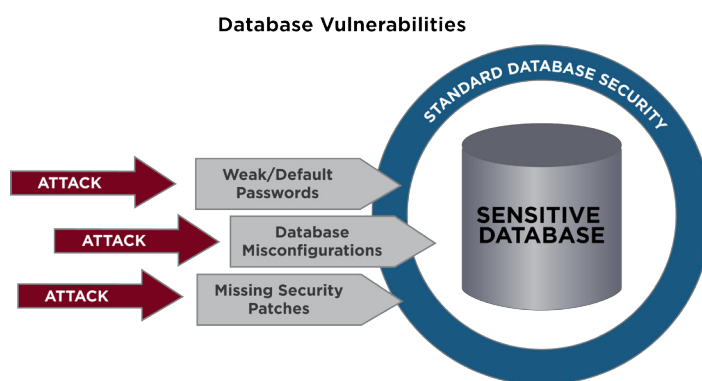
Step 2: Eliminate Vulnerabilities

Default and weak passwords, misconfigurations, and missing security patches provide avenues of attack to PHI. HIPAA specifies implementing policies and procedures to prevent, detect, contain, and correct security violations. It requires healthcare organizations to perform periodic technical evaluations in response to environmental and operational changes affecting PHI. DbProtect Vulnerability Management provides unparalleled database vulnerability assessment, allowing organizations to identify and eliminate vulnerabilities and fix misconfigurations that put their PHI at risk.

Vulnerability Management is driven by a powerful policy development engine that begins with a proven HIPAA compliant template. DbProtect's policy development is fed

by the SHATTER Knowledgebase, the most comprehensive and up-to-date vulnerability and threat knowledgebase in the industry. Each check in the SHATTER knowledgebase provides clear and detailed remediation instructions to insure that the vulnerabilities exposing PHI data are fixed in a timely manner.

DbProtect' Risk Analysis maps vulnerabilities to risk level and business impact. This helps organizations to prioritize their remediation plans and ensure the most serious threats to PHI are addressed quickly.

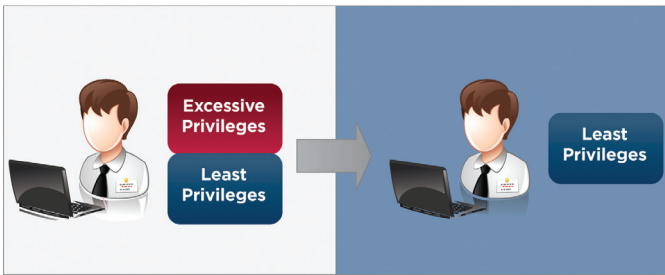


Step 3. Enforce Least Privileges

Over time, users accumulate more privileges than they need to do the job. This can lead to Segregation of Duties violations that enables an insider to make fraudulent changes or steal PHI. HIPAA specifically requires implementation of policies and procedures to ensure that all members of its workforce have appropriate access to PHI and to allow access to only those persons that have been granted access rights to PHI.

DbProtect Rights Management provides a detailed view of an organization's data ownership, access controls, and rights to sensitive information. Rights Management enables the organization to enforce the Principle of Least Privileges – grant only the privileges that users need to do their jobs. It allows you to restrict database access to a business need-to-know basis and mitigate against shared accounts. Rights Management also provides an audit trail on how privileges were granted, to help prevent against future privilege escalation.

Rights Management



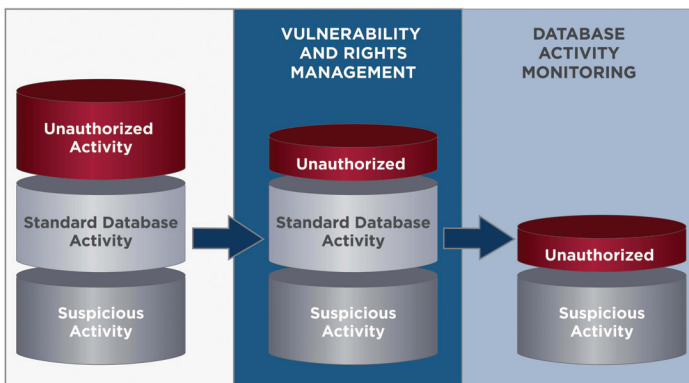
Step 4. Monitor for Deviations

HIPAA requires organizations to implement mechanisms that record and examine activity in info systems that contain PHI and to regularly test security systems and processes. DbProtect Database Activity Monitoring (DAM) meets HIPAA requirements by:

- Validating remediated vulnerabilities.
- Monitoring unremediated vulnerabilities to ensure they are not being exploited.
- Monitoring privileged user activity to ensure they are not engaged in any unauthorized behavior.
- Monitoring for any new avenues of attack.

DBProtect’s unique approach to Database Activity Monitoring (DAM) is precision monitoring. Precision monitoring employs DbProtect’s powerful policy development engine to streamline monitoring operations to focus on any suspicious activity threatening PHI. DbProtect’s precision DAM solution can be customized to a fine level of granularity – A specific activity, performed by a specific user, accessing specific data, in a specific database.

Precision DAM



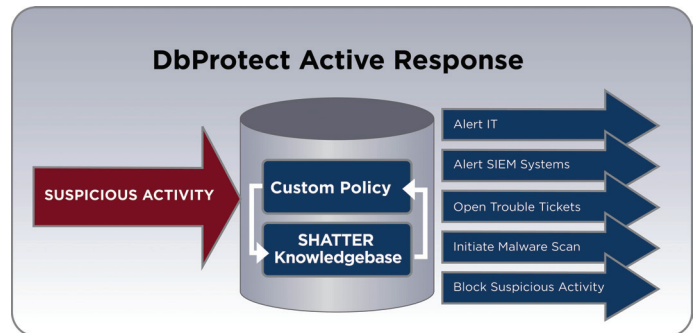
Backed by the same SHATTER knowledgebase that drives DbProtect Vulnerability Management, DbProtect DAM reduces risk and offers best-in-class data protection and HIPAA compliance reporting.

Step 5: Respond to Suspicious Behavior

DBProtect’s Active Response provides an additional layer of protection around Personal Health Information. Active Response can be configured to take action when an unauthorized and suspicious database activity is detected. Active responses can be customized to a fine level of granularity – A specific activity, performed by specific user, accessing a specific data, in a specific database.

For example: DbProtect’s SHATTER knowledgebase contains information on the latest SQL injection attacks. When DbProtect recognizes an SQL injection statement, Active Response can:

- Send an alert to IT Security.
- Notify the SIEM system to correlate database activity with web application logs.
- Initiate a malware scan to remove any injected code.



Incorporating a comprehensive and disciplined program of database security process control and address managing these five basic steps will help agencies to:

- Meet HIPAA compliance.
- Secure their databases and Personal Health Information.

OVERVIEW OF MANDATED HIPAA ADMINISTRATIVE SAFEGUARDS

While the Privacy Rule in HIPAA defines the standards for protecting all forms of personal health information (PHI), the Security Rule outlines specific Administrative and Technical Safeguards:

ADMINISTRATIVE SAFEGUARDS (164.308)	
Sections/Standard	The Application Security Solution
164.308 (a) (1) – Security Management Process <ul style="list-style-type: none"> - Risk Management - Risk Analysis 	For comprehensive risk management, DbProtect tracks, monitors and reports on all relevant data on information access and system events. All information is captured and retained in separate, secure data repository to maintain audit integrity.
164.308 (a) (4) – Information Access Management <ul style="list-style-type: none"> - Access Authorization - Access Establishment and Modification 	DbProtect provides a comprehensive analysis of which users have access to each system, which data and functionality they can access, and verification that the level of access that has been granted is appropriate based on the user's business function.
164.308 (a) (5) – Security Training and Awareness <ul style="list-style-type: none"> - Security Reminders - Protection from Malicious Software - Log-in Monitoring - Password Management 	DbProtect monitors the network and database user IDs to verify only one person is using the account and tests the password strength of all unique ID usernames and passwords accessing the database by importing a custom dictionary file of user-specified passwords into its Pen Test and Audit functionality.
164.308 (a) (6) – Security Incident Procedures <ul style="list-style-type: none"> - Response and Reporting 	DbProtect tracks, monitors and reports on all relevant data on information access and system events. All information is captured and retained in separate, secure data repository to maintain audit integrity. DbProtect, geared for the enterprise, allows IT and security personnel to set different alert levels based on activity type. These alerts can be intelligently filtered and disseminated in a variety of formats and to defined groups or individuals based on pre-established policies.
164.308 (a) (7) – Contingency Planning <ul style="list-style-type: none"> - Testing and Revision Procedure - Applications and Data Criticality Analysis 	DbProtect's alerting capabilities capture not only log-in attempts but also the highly detailed information necessary to support audit logs. DbProtect provides a solution for regularly scheduled and ad hoc database system testing to ensure regulatory compliance.
164.312 (a) (1) – Access Controls <ul style="list-style-type: none"> - Unique User identification 	DbProtect assesses database security both from the outside and the inside by checking for denial of service and password attacks, misconfigurations, vulnerabilities, identification/password and access control issues, and application and operating system integrity weaknesses. For HIPAA compliance, organizations are required to have in place a continuous monitoring and auditing solution that tells them who is accessing data and what happens to the data. DbProtect's Audit and Threat Management module is a key requirement of HIPAA and adheres to the requirements of continuous monitoring, tracking access to data, collection all privileged user activity and events, enforcing segregation of duties, and regular reporting. DbProtect's Rights Management restricts access to data by "need to know" and further identifies unnecessary accounts, test accounts, and custom application accounts needed for removal.
164.312 (b) – Audit Controls	DbProtect's Asset Management module audits databases and provides a complete inventory of databases that customers can use to classify if the database is compliant.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

Follow us on Twitter: [www.twitter.com/appsecinc](https://twitter.com/appsecinc) | [www.twitter.com/teamshatter](https://twitter.com/teamshatter)

**APPLICATION
SECURITY, INC.**[®]
www.appsecinc.com