IDERA® | SQL Security Solution Brief

SECURITY AND COMPLIANCE SOLUTIONS FOR HIPAA

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to, among other things, develop regulations that protect the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes standards for privacy controls involving health information, dubbed protected health information (PHI). The Security Rule establishes standards for security controls involving electronic PHI that directly impacts database security in the enterprise. Furthermore, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 contains specific incentives designed to accelerate the adoption of electronic health record systems among providers as well as more enhanced controls around the original HIPAA Security Rule including new breach notification and enforcement requirements.

In 2013, a new set of HIPAA-related requirements called the Omnibus Rule was enacted to further strengthen the HIPAA and HITECH controls. The biggest changes brought about by the Omnibus Rule related to information privacy and security were a requirement that all business associates and their subcontractors must now follow the HIPAA and HITECH requirements as a traditional “covered entity” would. The Omnibus Rule also brought about an increase in civil penalties related to non-compliance.

In order to define the proper HIPAA requirements baselines, audit database object/data changes, and report the appropriate database privacy and security-related findings to auditors and regulators, you must be able answer the following questions:

1. **Who has access to my electronic PHI, and how do I audit the activity?**
2. **How do I define a secure baseline and maintain it across my SQL Server environment?**
3. **How can I implement repeatable processes to help maintain the security standards?**
4. **How do I audit permissions, logins, and object and data changes on my SQL Server?**
5. **What is the best way for me to ensure not only ongoing compliance with the HIPAA, HITECH, and Omnibus Rule regulations but also help maintain reasonable security across my SQL Server databases?**

HOW DOES SQL SECURE ADDRESS THESE REQUIREMENTS?

A key course of action to comply with HIPAA is developing, maintaining and enforcing internal controls and procedures for your IT environment. IDERA SQL Secure is a necessary tool for establishing the right controls to meet those regulations. SQL Secure is a security analysis and management solution that helps IT and security administrators and managers identify Microsoft SQL Server security access violations and ensures that security policies are enforced. You can find out who has access to what and identify each user's effective rights across all SQL Server objects. Furthermore, you can also alert on violations of your corporate policies, and secure your environment (internally and externally) from the most common methods of intrusion.

SQL Secure helps IT organizations address the requirements of the HIPAA security standards where they apply to SQL Server. SQL Secure helps you to define your SQL Server baselines by providing a customizable IDERA-defined template (HIPAA Guidelines for SQL Server), which provide a "realistic" guideline for establishing the appropriate security checks for your environment. In addition, it can also extract your permissions and settings from any point in time and identify any changes or vulnerabilities that may exist. This gives you the power to proactively address these exceptions before reports are delivered to your auditors.

HOW DOES SQL COMPLIANCE MANAGER ADDRESS THESE REQUIREMENTS?

SQL Compliance Manager is a comprehensive Microsoft SQL Server auditing solution that uses policy-based algorithms to track changes to your SQL Server objects and data. SQL Compliance Manager provides continuous auditing of all SQL Server activity by identifying who did what, when, how and whether the event is initiated by privileged users or hackers. SQL Compliance Manager goes beyond traditional auditing approaches by providing custom real-time monitoring and auditing of all data access, updates, schema modifications and permission changes. Audited data is collected and securely stored for forensic analysis and reporting. It also provides tamper-proof data security features as well as methods for watching events without exposing account information. Additionally, SQL Compliance Manager provides a robust alerting engine that contains counters and trend graphs to identify activity level deviations often associated with suspect activities. Such visibility into your SQL Server database environment helps ensure ongoing compliance with the existing HIPAA-related security standards and scale to meet security best practices moving forward.

HIPAA Citation	Requirement	IDERA SOLUTION
164.306 (a) (1)	**Security Standards** Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.	**SQL Secure** extracts the SQL Server permissions and ensures that the right employees have access to the data and identifies any changes that have been made to the established baselines which ensures integrity, confidentiality and availability.
164.306 (a) (2)	**Security Standards** Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	**SQL Secure** establishes security checks that protect against anticipated threats and ensures that those checks are implemented and consistent across the SQL Server environment.
164.306 (b,1)	**Security Standards** Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	**SQL Compliance Manager** and **SQL Secure** together help to establish solid standards and auditing procedures (auditing, security checks, reporting).
164.308 (1,i)	**Security Management Process** Implement policies and procedures to prevent, detect, contain and correct security violations.	**SQL Secure** helps to define the right permissions to help prevent unauthorized user accesses. **SQL Compliance Manager** audits all SQL Server activity and helps to detect abnormal access to the data.
164.308 (A)	**Risk Analysis** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity.	**SQL Secure** stores the SQL Server permissions, establishes a baseline for the entire environment to ensure that potential risks and vulnerabilities are reduced and also ensures that the right personnel have access to the SQL Server objects.
164.308 (B)	**Risk Management** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306 (a).	**SQL Secure** provides a HIPAA guideline that is based on STIG & CIS standards. These security checks align with the industry standards which help to reduce risks and SQL Server vulnerabilities.
164.308 (D)	**Information System Activity Review** (Required). Implement procedures to regularly r eview records of information system activity such as audit logs, access reports and security incident tracking reports.	**SQL Compliance Manager** provides auditing for all SQL Server activity, including login access (successful/failed) and provides tracking reports to prove it.

HIPAA Citation	Requirement	IDERA SOLUTION
164.308 (3,i)	**Standard: Workforce Security** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	**SQL Secure** helps IT security professionals establish the right policies to ensure that workforce members have the appropriate access to SQL Server as well as identify employees who should not have access to health information.
164.308 (3,C)	**Termination procedures** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.	**SQL Secure** helps SQL Server administrators confirm that a terminated employee no longer has access to the SQL Server objects. **SQL Compliance Manager** tracks all database access activity. When an employee's access is removed, the task is captured and stored in our repository and also provides the reports to prove it.
164.308 (5) (C)	**Implementation Specifications.** Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	**SQL Compliance Manager** audits all login activity which includes both failed & successful for any user and additionally provides customizable reports.
164.308 (7) (i) (ii) (A,B,C,D,E)	**Implementation Specifications.** **Standard: Contingency Plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (ii) **Implementation specifications:** (A) **Data backup plan (Required).** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) **Disaster recovery plan (Required).** Establish (and implement as needed) procedures to restore any loss of data. (C) **Emergency mode operation plan (Required).** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) **Testing and revision procedures (Addressable).** Implement procedures for periodic testing and revision of contingency plans. (E) **Applications and data criticality analysis (Addressable).** Assess the relative criticality of specific applications and data in support of other contingency plan components.	**SQL Safe Backup** provides high-performance backup and recovery solutions for Microsoft SQL Server. **SQL Safe Backup** offers unique policy based management which enables DBAs to define and automate backup, restore and log shipping policies across multiple servers and databases. This aids in developing the right contingencies for data recovery. These policies can be used for: • Data backup plans • Disaster recovery plans • Emergency mode operation • Testing and revision procedures • Application and data criticality analysis

HIPAA Citation	Requirement	IDERA SOLUTION
164.312 (a,1)	**Technical Standard:** **Access control**. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308 (a) (4).	**SQL Secure** allows you to define baselines for accessing SQL Server data, ensuring that the right person or logins have the right permissions to the right SQL Server objects. Changes to a login or permission (grant/revoke) can be easily identified with an assessment.
164.312 (b)	**Technical Standard:** **Audit controls**. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	**SQL Compliance Manager** audits all activity to the SQL Server database and stores that information in a tamper-proof repository.
164.404 (a) (1) (2)	**Security and Privacy - General rule**. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. **Breaches treated as discovered.** For purposes of paragraph (a) (1) of this section, §§ 164.406 (a), and 164.408 (a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	**SQL Compliance Manager** gives the covered entity the ability to discover the breach of unsecured "protected health information" with the sensitive column auditing feature. Any combinations of columns can be audited for breach identification. **SQL Compliance Manager** addresses the burden of proof with detailed reporting out of the box.

HIPAA Citation	Requirement	IDERA SOLUTION
164.404 (c) (1) (A),(B)	**Security and Privacy** - (c) **Implementation specifications:** **Content of notification**- (1) Elements. The notification required by (a) of this section shall include, to the extent possible: (A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information.	**SQL Compliance Manager** identifies the content of the breach: date, time, data accessed and by whom and by the exact name of the column(s) that were accessed (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved)
HITECH 13402 (a) (f), (1), (2)	**Notification In the Case of Breach** (a) **In General.**—A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. (f) **Content of Notification**.—Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following: (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known. (2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).	**SQL Compliance Manager** addresses auditing of the protected health information and captures who has accessed that information and additionally provides a clear audit trail: (such as full name, Social Security number, date of birth, home address, account number, or disability code or any column or groups of columns within the audited table. SQL Compliance Manager also provides alerting to the appropriate person when the PHI data is accessed.

IDERA understands that IT doesn’t run on the network – it runs on the data and databases that power your business. That’s why we design our products with the database as the nucleus of your IT universe.

Our database lifecycle management solutions allow database and IT professionals to design, monitor and manage data systems with complete confidence, whether in the cloud or on-premises.

We offer a diverse portfolio of free tools and educational resources to help you do more with less while giving you the knowledge to deliver even more than you did yesterday.

Whatever your need, IDERA has a solution.

IDERA