

## Security and Compliance Solutions for Health Insurance Portability and 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 develop regulations protecting the privacy and security of certain health information.<sup>1</sup> 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 national standards for the protection of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. Furthermore, the Health Information Technology for Economic and Clinical Health Act (HITECH) contains specific incentives designed to accelerate the adoption of electronic health record systems among providers. In order to define the right baselines and audit database object/data changes, and report those findings to auditors, you must be able answer the following questions:

1. Who has access to my "HIPAA" data and how do I audit the activity?
2. How do I define a secure baseline and maintain it across my SQL Server enterprise?
3. How can I implement repeatable processes to help maintain my standards?
4. How do I audit permissions, logins, object and data changes on my SQL Server?
5. What is the best way for me to comply with HIPAA-HITECH regulations with regards to my SQL Server databases?

### How Does SQLsecure Address These Requirements?

Idera SQLsecure is a security analysis solution that helps IT organizations identify SQL Server security 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.

A key course of action to comply with HIPAA-HITECH is developing, maintaining and enforcing internal controls and procedures for your IT environment. SQLsecure is a necessary tool for establishing the right controls to meet those regulations.

SQLsecure helps IT organizations address the requirements of HIPAA-HITECH where they apply to Microsoft SQL Server. SQLsecure helps you to define your SQL Server baselines by providing three Idera defined templates (**Level-1 Basic**, **Level-2 Balanced**, **Level-3 Strong**) which provide "realistic" guidelines 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 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.

#### Confidential and Proprietary

## SUMMARY

HIPAA Citation	Description	Idera Compliance
164.306 (1)	<p><b>Security Standards</b> Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.</p>	<p><b>SQLsecure</b> 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.</p>
164.306 (2)	<p><b>Security Standards</b> Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.</p>	<p><b>SQLsecure</b> establishes security checks that protect against anticipated threats and ensures that those checks are implemented and consistent across the SQL Server environment</p>
164.306 (4,b,1)	<p><b>Security Standards</b> 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</p>	<p><b>SQL compliance manager</b> and <b>SQLsecure</b> together help to establish solid standards and auditing procedures (auditing, security checks, reporting)</p>
164.308 (1,i)	<p><b>Security Management Process</b> Implement policies and procedures to prevent, detect, contain and correct security violations</p>	<p><b>SQLsecure</b> 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</p>
164.308 (A)	<p><b>Risk Analysis</b> 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.</p>	<p><b>SQLsecure</b> 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 has access to the SQL Server objects</p>
164.308 (B)	<p><b>Risk Management</b> Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).</p>	<p><b>SQLsecure</b> provides three realistic security checks that are based on STIG, CIS &amp; DISA standards. These security checks exceed the industry standards which help to reduce risks and SQL Server vulnerabilities</p>

### Confidential and Proprietary

## SUMMARY

HIPAA Citation	Description	Idera Compliance
164.308 (D)	<b>Information System Activity Review</b> (Required). Implement procedures to regularly review records of information system activity such as audit logs, access reports and security incident tracking reports.	<b>SQL compliance manager</b> provides auditing for all SQL Server activity, including login access (successful and failed) and provides tracking reports to prove it
164.308 (3,i)	<b>Standard: Workforce Security</b> 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.	<b>SQLsecure</b> can help IT security professionals establish the right policies that ensure that workforce members have the appropriate access to SQL Server and also assess the changes as well as employees who should not have access to health information
164.308 (c)	<b>Termination procedures</b> Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends.	<b>SQLsecure</b> helps SQL Server administrators to confirm that a terminated employer no longer has access to the SQL Server objects. <b>SQL compliance manager</b> tracks all permission activity. When an employee's access is removed, <b>SQL compliance manager</b> captures the information in our repository and also provides the reports to prove it.
164.312 (a,1)	<b>Technical Standard:</b> Access control	<b>SQLsecure</b> tracks changes to SQL Server permissions and also helps to define the right security check baseline
164.312 (b)	<b>Technical Standard:</b> Audit controls	<b>SQL compliance manager</b> audits any all activity to the SQL Server database and stores that information in a tamper-proof repository.

### Confidential and Proprietary