Enhanced Compliance for HIPAA in Applications, Databases and Middleware

WHITE PAPER

Table of Contents

Executive Summary

Two decades after it was signed into law the Health Insurance Portability and Accountability Act (HIPAA) remains a challenge for many organizations. Whether the penalty is simply financial or if it also involves a severe hit to the reputation, the law continues to strike fear into many healthcare providers and compliance professionals.

HIPAA compliance requires a conscientious, diligent staff that is well-trained on the nuances of the law. It also requires solid processes. And while good processes and meticulous documentation are necessary for compliance they are certainly not sufficient. In the realm of ePHI (electronic protected health information), compliance enforcement requires software that is purpose-built to control access, timing and scope of changes to sensitive applications and databases.

Orca is an application configuration automation and compliance enforcement solution that 1) automatically detects then corrects non-compliant configurations, 2) centrally secures and controls application, database and middleware configuration changes and 3) provides compliance audit trails indicating the nature, timing, locations and approvers behind each change.

Business Critical Applications Updates: Progress & Peril

Each revision to your business critical application represents progress. Those application updates allow it to deliver more value to more users and more use cases. But those same changes, whether from well-intentioned employees or trusted contractors can also represent a profound business risk. Certainly most software and middleware configuration changes are executed without negative consequences. But hackers and other intruders only need to be successful once. And regulatory bodies are keen to make an example of organizations that did not do everything in their power to protect demographic and health information.

Common Approaches: People, Process & Technology

The HIPAA Security Checklist in this document is intended to control those risky changes with a mix of people, process and technology approaches.

People and Process:

Hiring competent, experienced staff and supporting them with ongoing training is a very common and very necessary approach. Developing a set of repeatable processes around the creation and handling of sensitive health information is also essential.

Technology:

But even the most professional, well-trained, well-intentioned staff may inadvertently deploy changes to the environment which might cause related applications, databases and middleware to drift out of compliance. As these non-compliant changes ripple through your ecosystem, the results can lead to unpredictable outcomes including outages, performance problems and security breaches. People and process approaches are not enough. IT staff needs a technology solution to enforce and ensure compliance.

Knowing this, many organizations attempt to build their own solutions or repurpose tools built for other use cases to assist them with controlling configuration changes to their sensitive applications and databases. Over time these spreadsheets, SharePoint sites, scripting and even homegrown tools can become unreliable and unwieldly "Franken-tools", requiring special skills just to operate and maintain. Hiring for this unique skill set creates its own challenges as well.

> *IT teams, their employers and the customers who entrust them with protected health information deserve better.*

In summary, technological approaches to securing ePHI need more than firewalls, data encryption and access control to applications and data. A full HIPAA technology portfolio should also provide for central, secure control of application, database and middleware *configurations*. Automated, enforced change control down to the configuration level is key to preventing intentional or inadvertent breaches of business critical applications and databases.

How Orca Addresses HIPAA Requirements

Orca centrally controls changes: including *what* changes are made, *when* they are made, *where* they are applied and even *who* can *view, edit and approve* those changes.

Even before those application and database configuration changes are applied, Orca users "Preview" and "Dry Run" intended changes to validate that configuration changes will be successful and will be applied to intended nodes.

Unlike a simple PowerShell script that can indiscriminately apply system-wide changes without central console-level oversights or rollbacks, Orca is an application configuration automation and compliance solution that centrally controls the changes that are capable of introducing HIPAA security vulnerabilities. Because of its central control and its intelligent workflow automation, Orca eliminates the need for direct access to servers, a major source of uncontrolled IT changes.

Afterwards, Orca users with access privileges can view the change audit logs that display the "who", "what", "why", "when" and "where" behind those changes.

Summary

While there are no "magic bullets" or guarantees when it comes to HIPAA compliance, this paper and the table below are meant to highlight how Orca can tilt the odds in your favor by enhancing your ability to enforce change control in your sensitive applications and databases. The following table maps Orca capabilities against several key HIPAA security criteria. Please use it to assist you in addressing previously un-addressable gaps in your HIPAA Compliance efforts.

HIPAA Security Checklist

HIPAA SECURITY RULE REFERENCE	SAFEGUARD	How Orca supports each safeguard
Administrative Safeguards		
164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking?	Orca provides audit trails and access reports for the environments that it manages.

164.308(a)(2)	Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	A security official can be assigned by an administrator in Orca.
164.308(a)(3)(i)	Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, 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 (EPHI).	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed?	Orca employs a robust role based access control (RBAC) system that controls which individuals and groups have view, edit or approve privileges. These privileges can be set to restrict at granular levels who has access to specific applications and locations.
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine that the Access of an employee to EPHI is appropriate?	Orca employs a robust role based access control (RBAC) system that controls which individuals and groups have view, edit or approve privileges. These privileges can be set to restrict at granular levels who has access to specific applications and locations.
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves your organization or as required by paragraph (a)(3)(ii)(B) of this section?	Orca's RBAC system allows administrators to disable access for terminated employees.
164.308(a)(4)(i)	Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process?	Orca's RBAC system allows users to easily add groups to access managed systems.
164.308(a)(5)(i)	Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords?	Orca integrates with industry standard tools for managing user accounts and passwords, such as MS Active Directory.
164.308(a)(6)(i)	Security Incident Procedures: Implement policies and procedures to address security incidents.	

164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or know security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes?	Orca's application configuration compliance heat map graphically indicates any out of compliance nodes. Orca manages your security compliance policy for infrastructure configurations. And Orca notifies and remediates violations of your security compliance policy.
164.308(a)(7)(i)	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 EPHI.	
164.308(a)(7)(ii)(C)	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode?	Easily take infrastructure configurations from one environment to a disaster recovery environment to ensure that critical applications continue to run.
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans?	Orca can be set to push configuration changes from Production to a DR environment periodically to ensure infrastructure continuity in emergency mode.
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components?	Orca administrators can define the criticality of applications and environments and how they are managed.
Technical Safeguards		
164.312(a)(1)	Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity?	Each user is uniquely defined in Orca. Orca audit trails identify the user that initiated or approved a change.
164.312(c)(1)	Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner?	Within the Orca solution the ability to view, edit or approve configuration changes can be granted to named individuals or to job classifications and functions.

		Orca can also be used to control access to system components that are linked to individual users.
164.312(e)(1)	Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of?	Uses of and changes to identification and authentication mechanisms are tracked by Orca's RBAC. Changes, additions or disabling of accounts with root or administrative privileges are also tracked and logged by Orca.

About the authors:

Timothy Wall brings over 20 years of business experience in both large established and early stage companies to his role as co-founder and CEO of Trifectix. Prior to Trifectix, Tim was co-founder and CEO of VaraLogix, an innovative deployment automation solution provider acquired by BMC Software. Previously, he served as the initial CFO for several early stage software companies in Austin, including Innography and CoreTrace while also being an active angel investor. From 2001 to 2006 Tim served as co-founder and CFO of BuildForge, a build process automation solution company, through to its acquisition by IBM. Prior to BuildForge Tim worked as a manager in financial planning for the Playboy Entertainment Group and as a Financial Analyst with the Warner Music Group. Tim holds an MBA in Finance from the University of Southern California and a B.S. in Finance from California State University – Northridge.

Robin Fuller is a co-founder of Trifectix and Chief Software Architect of Orca, the company's flagship application configuration automation and compliance solution. Prior to Trifectix, Robin co-founded VaraLogix which was later acquired by BMC Software as part of their application deployment and DevOps portfolio. Earlier in his career, Robin spent stints in healthcare IT and he was a Senior Software Engineer for IBM/ BuildForge.
Robin holds degrees in Mathematics and Engineering from Trinity College in Dublin.

completeness of the information. To the extent permitted by applicable law, Trifectix provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will Trifectix be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if Trifectix is expressly advised in advance of the possibility of such damages. Trifectix does not provide legal advice. No software product referenced herein serves as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order, executive order, and so on (collectively, “Laws”) referenced herein or any contract obligations with any third parties. You should consult with competent legal counsel regarding any such Laws or contract obligations.”