TECH BRIEF

How HIPAA Compliance is Impossible without Privileged Management

Written by Joseph Grettenberger, compliance risk advisor, Compliance Collaborators, Inc.

Introduction

For many organizations, compliance with data security standards doesn't seem to be getting easier. IT security compliance efforts are forever competing with ever-pressing information security threats, operational vulnerabilities and daily business risks, and often lose out in the battle for resources and funding.

However, the reality is that these areas do not have to compete. By implementing proven solutions that address multiple foundational controls, you can achieve and prove regulatory compliance while guarding against the risks that threaten everyday operations or even land organizations in the headlines. For example, a key component of regulatory compliance is implementing (and demonstrating that you have implemented) reasonable and appropriate IT-related internal safeguards that minimize the risk of unauthorized disclosures and data breaches. Achieving and proving your compliance with such mandates requires you to mitigate the security risk of system users obtaining privileged but unauthorized access to sensitive data — and implementing these privileged management controls will also further your organization's broader security goals.

In this paper, you'll learn about IT security compliance for the Health Insurance Portability and Accountability Act (HIPAA) from an auditor's perspective. Although HIPAA represents only a portion of the data security compliance obligations faced by most organizations handling healthcare data, it is one of the most significant. For information about other mandates intended to protect sensitive data, please see my related papers on the Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley Act (SOX).

Health Insurance Portability and Accountability Act

Entities subject to HIPAA

The Health Insurance Portability and Accountability Act was signed into law on August 21, 1996, adding a new Part C to Title XI of the Social Security Act (sections 1171–1179). One of the most important provisions of HIPAA is the mandatory safeguarding of all recorded personal health information (PHI), including PHI stored in an electronic form (ePHI).

The reach of HIPAA's provisions for safeguarding PHI was extended under the Health Information Technology for Economic and Clinical Health (HITECH) Act on February 17, 2009, and again on January 25, 2013, in HIPAA's omnibus final rule. In particular, HITECH extended HIPAA's traditional requirements to "business associates" of "covered entities" (see Subtitle D, Section 13401). Covered entities include hospitals, medical billing centers, health insurance companies, healthcare clearinghouses and other health care providers. HIPAA's omnibus final rule expanded HITECH's already broad "business associates" category, which included health information exchange organizations, e-gateways handling ePHI and vendors assisting a covered entity with personal health records, to also include subcontractors that create, receive, maintain or transmit protected health information on behalf of a business associate.

What HIPAA requires from organizations

Organizations subject to HIPAA are required to:

- Ensure the confidentiality, integrity, and availability of all electronically protected health information created, received, maintained, or transmitted
- Regularly review system activity records, such as audit logs, access reports, and security incident tracking reports
- Establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process containing ePHI
- Monitor login attempts and report discrepancies
- Identify, respond to, and document PHI breach incidents, as well as properly notify specified parties

While the databases of EHR systems are obvious areas where ePHI subject to HIPAA resides, there are many other systems where ePHI may be stored or transmitted.

In addition, under HITECH Subtitle D, Section 13402 (e)(2), and HIPAA's final omnibus rule, virtually all organizations that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose ePHI must also comply with rigorous breach notification requirements when PHI is compromised. For example, if the number of people affected by a data privacy breach is more than 500 for a given state or jurisdiction, the media must be notified.

Systems subject to HIPAA

While the databases of electronic health record (EHR) systems are obvious areas where ePHI subject to HIPAA resides, there are many other systems where ePHI may be stored or transmitted. These systems include personal medical devices, modern medical equipment, tablets, cell phones, copiers, scanners, fax machines, multi-function devices, print servers, ePHI databases, encrypted email, voice mail servers, security camera systems, protected file servers, network shared drives, and local machines such as desktops and laptops.

These adjunct areas of ePHI storage may not be addressed by the organization's security policies, but HIPAA compliance requires they be properly protected.

Penalties for violations

The Office of Civil Rights (OCR), a division of Health and Human Services (HHS), enforces HIPAA compliance and investigates suspected breaches. In recent years, the OCR has imposed fines through settlements against providers who have failed to take reasonable and appropriate safeguards to protect their ePHI. Table 1 lists the current maximum penalty amounts per violation and per individual provision of the HIPAA Security, Privacy and Breach Notification rules. Since organizations can be in violation of multiple provisions of multiple rules, OCR fines can and have exceeded $1,500,000.

One Identity's privileged management solutions

The security features of primary applications are insufficient.

Twelve of the 18 standards in HIPAA's Security Rule, especially §164.308(a)(4), §164.308(a)(5) and §164.312(a)(1), contain requirements that emphasize the need for organizations to have basic privileged access management controls that limit access to ePHI and ensure that each system user is uniquely identified with access that is explicitly approved by authorized persons. These requirements apply across the entire organization to all systems creating, transmitting, storing or accessing ePHI.

Therefore, using the group permissions and role-based management features of EHRs and other vendor applications (radiology information systems, picture archiving and communication systems, practice

Violation category — Section 1176(a)(1)1	Each violation	Maximum penalty of all such violations of an identical provision in a calendar year
(A) Did Not Know	$100 – $50,000	$1,500,000
(B) Reasonable Cause	1,000 – 50,000	1,500,000
(C)(i) Willful Neglect—But Later Corrected	10,000 – 50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

Table 1. Penalties for HIPAA violations (Source: Federal Register Vol. 78, No. 17, p. 5583)

management systems and so on) is not enough to adequately safeguard an organization’s ePHI — organizations also need to protect ePHI stored on and transmitted by support systems (such as file servers, mail servers, backup servers, development and test servers, and network devices) and underlying platforms (including databases, operating systems, hypervisors and VM hosts).

One Identity's privileged account management solutions automate many of the safeguards required by today’s IT security mandates while also providing foundational IT security measures.

Automating privileged account management and streamlining compliance

One Identity privileged account management (PAM) solutions automate many of the safeguards required by today’s IT security mandates while also providing foundational IT security measures. For example, the three One Identity PAM solutions highlighted in this paper address requirements for IT general controls (ITGCs) not only for 12 of the 18 standards in HIPAA’s Security Rule, but also for all five internal control components of SOX, six of the 12 PCI DSS requirements, and 28 of the 35 control objectives in ISO 27001, Annex A.

Specifically, One Identity PAM solutions enable organizations to:

- Substantially automate the enforcement of privileged account management, including requests, reviews, approvals, denials and revocations
- Quickly respond to management, audit and government inquiries with reports that demonstrate historical compliance with many information security policies and procedures
- Monitor and report on privileged activities, including those during sensitive time periods or outside the course of normal business operations
- Substantiate evidence of policy violations using a separate database of activity records, such as when personnel sanctions related to the security of information systems need to be applied

A more complete and effective solution

In short, One Identity privileged account management solutions – such as One Identity Safeguard – are designed to continuously manage routine and non-routine privileged access to the platforms and environments supporting critical applications and housing sensitive data — filling a critical security gap for traditionally weak administrative and technical safeguards. The solutions equip organizations to adopt robust privileged account management and monitoring practices that augment and to some extent preempt standard user activity monitoring, malware and intrusion detection controls.

While not a replacement for network monitoring tools, when regularly used as part of an information system change management program, One Identity PAM solutions can greatly reduce a host of unauthorized access and system changes — including unauthorized access to sensitive data, unauthorized system configuration changes, unauthorized software downloads and more — thereby preventing many policy violations before they happen.

By enabling controlled use of administrative privileges, ensuring controlled access based on need-to-know, and providing detailed recordings of discrete activities performed in controlled environments, One Identity PAM solutions help organizations not only control privileged access to their production operating environments but ensure that critical access controls are applied to security architectures that are anticipated in all phases of the system development life cycle. The One Identity privileged management solutions discussed in this paper are:

- One Identity Safeguard for Privileged Passwords
- One Identity Safeguard for Privileged Sessions
- Privilege Manager for Sudo

One Identity Safeguard for Privileged Passwords

Safeguard for Privileged Passwords automates controls and secures the entire process of granting administrators the credentials necessary to perform their duties. It ensures that administrative or privileged access is granted according to established policy, with appropriate approvals; that all actions are fully audited and tracked; and that the password is changed immediately upon its return.

Safeguard for Privileged Passwords also eliminates the security exposure posed by embedded privileged passwords required for applications to talk to each other or to databases by replacing these hardcoded passwords with programmatic calls that dynamically retrieve the account credentials. Safeguard for Privileged Passwords is deployed on a secure, hardened appliance.

One Identity Safeguard for Privileged Sessions

Safeguard for Privileged Sessions enables authorized, trusted workforce members to issue privileged access for a specific period or session to administrators, remote vendors and high-risk users — with full recording and replay for auditing and compliance. It provides a single point of control from which trusted workforce members can authorize connections, limit access to specific resources, allow only certain commands to be run, view active connections, record all activity, alert if connections exceed pre-set time limits, and terminate connections.

This solution is also deployed on a secure, hardened appliance and when combined with Safeguard for Privileged Passwords, it can completely hide the account password from the privileged user.

One Identity Privilege Manager for Sudo

Privilege Manager for Sudo enhances sudo with a central policy server that enables centralized management of sudo and the sudoers policy file, as well as centralized reporting on sudoers access rights and activities. It also performs keystroke logging, complete with search and playback capabilities, for in-depth auditing and compliance requirements. Privilege Manager for Sudo is part of the Privileged Access Suite for UNIX.

> When regularly used as part of an information system change management program, One Identity PAM solutions can greatly reduce a host of unauthorized access and system changes — thereby preventing many policy violations before they happen.

Mapping HIPAA standards to One Identity PAM solutions

This section provides a detailed mapping of IT-related HIPAA requirements to the capabilities of One Identity's privileged account management solutions. The requirements are sorted by relevant HIPAA Security Rule standards and related implementation specifications to help your organization review its ePHI safeguards for possible gaps in compliance.

Administrative safeguards

HIPAA standard and related implementation specifications		**How One Identity PAM solutions help**
§164.308(a)(1)(i) Security Management Process		Under HIPAA, covered entities and business associates must implement minimum reasonable security management safeguards to mitigate risk throughout their entire ePHI environment. One Identity PAM solutions enable organizations to automate or partially automate procedures and enforce policy designed to prevent, detect and contain potential security violations related to excessive ePHI access privileges in systems outside EHRs and in underlying platforms that store or protect ePHI.
§164.308(a)(1)(ii)(A) Risk Analysis (R)	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 or business associate.	When the organization is responding to risk assessments, inquiries and audits of administrative and technical safeguards around IT systems and network infrastructure, One Identity PAM solutions can address questions concerning access requests, permissions granted and inappropriate ePHI access, as well as help the organization demonstrate that it uses unique user IDs and sufficiently secure password management settings. Specifically, **Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** can: • Show privileged activities in systems where ePHI is stored locally • Identify remote sessions to systems identified as containing or accessing ePHI • Detail server and privileged user info • Identify ePHI access parameters such as Account policies and Administrator Access by Computer
§164.308(a)(1)(ii)(C) Sanction Policy (R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Having defensible evidence is vital when applying workforce member sanctions. **Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** can be configured to record or log all activity, especially in Windows environments. These recordings are designed to prevent much of the log tampering seen with security and privacy incidents and policy violations. In short, these tools can be used to audit and securely report evidence of workforce member non-compliance with the organization's access control security policies.

HIPAA standard and related implementation specifications		**How One Identity PAM solutions help**
§164.308(a)(1)(ii)(D) Information System Activity Review (R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** all record or log system activities of those with privileged access, including: • Unauthorized email access • Administrator logon activity • Unauthorized use of service accounts • Administrator access to files and other objects • Access to audit logs • Access to health records and related files • Security incidents
§164.308(a)(3)(i) Workforce Security		
§164.308(a)(3)(ii)(A) Authorization and/or Supervision (A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** help ensure that access privileges are authorized in systems that store or protect ePHI beyond EHRs. In particular, they ensure that an authorization workflow is used to require approvals for requests for: • Privileged accounts with access to ePHI • Privileged sessions with access to ePHI For workforce member supervision, **Safeguard for Privileged Sessions** can be used to monitor privileged user activity as it happens or for later reviews and audits. Privilege Manager for Sudo's keystroke logging feature enables organizations to review privileged access on UNIX and Linux systems.
§164.308(a)(3)(ii)(B) Workforce Clearance Procedure (A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Determining appropriateness of access should happen at all points of the privileged account lifecycle. **Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for UNIX** can help organizations establish, manage and enforce predefined privileged account access levels, requests for privileged access and access authorization workflows. In addition, the access reports in these solutions can be used to implement a procedure for periodic attestation reviews to continually ensure appropriate access.

HIPAA standard and related implementation specifications		How One Identity PAM solutions help
§164.308(a)(3)(ii)(C) Termination Procedures (A)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** can quickly terminate privileged access to all systems containing ePHI by disabling an individual's user ID — even if that user has access to multiple systems, perhaps as a result of holding multiple roles over years of employment. Because end users do not use static passwords with these solutions, they never have permanent access to their login credentials. This makes user account deprovisioning across all systems managed by these solutions as simple as a one-step procedure of removing their access to the password vault.
§164.308(a)(4)(i) Information access management		
§164.308(a)(4)(ii)(A) Isolating health care clearinghouse functions (R)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** can provide safeguards to isolate and protect a clearinghouse function from the larger organization by: • Preventing direct access to health care clearinghouse systems from other business units • Enforcing limited access authorization of properly approved privileged access requests (if policy permits such access by the larger organization) using an authorization request approval workflow • Recording every session for which authorization is granted
§164.308(a)(4)(ii)(B) Access Authorization (A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** all enable centralized management (review, approval and monitoring) of access requests to systems containing ePHI. Granular privilege authorization controls enable organizations to enforce policies for granting least-privilege access to ePHI on many operating platforms, including Windows, OSX, and a wide variety of UNIX and Linux systems. The activity review capabilities of each solution can provide information on who was granted access to what system, when access was granted and for how long, and what commands were run.
§164.308(a)(4)(ii)(C) Access Establishment and Modification (A)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	**Safeguard for Privileged Passwords** and **Safeguard for Privileged Sessions** enable organizations to establish, document, review and modify outdated access privileges. Moreover, they greatly reduce the amount of privileged access review work required by permitting trusted roles to issue passwords with expiration dates and times according to the organization's maximum password age policy.

HIPAA standard and related implementation specifications		**How One Identity PAM solutions help**
§164.308(a)(5)(i) Security Awareness and Training		
§164.308(a)(5)(ii)(B) Protection from Malicious Software (A)	Procedures for guarding against, detecting and reporting malicious software.	**Safeguard for Privileged Passwords** and **Safeguard for Privileged Sessions** can greatly reduce the likelihood of malware spreading in an organization's network. For example, proper privilege management can guard against malware with the use of randomized and constantly changing passwords, which reduces the chance for man-in-the-middle attacks like credential interception, password hash forwarding and ePHI transmission interception. In addition, users are not given direct access to systems but instead go through a proxy, which reduces the risk that an infected workstation can spread malware to other systems.
§164.308(a)(5)(ii)(C) Log-in Monitoring (A)	Procedures for monitoring log-in attempts and reporting discrepancies.	**Safeguard for Privileged Passwords** and **Safeguard for Privileged Sessions** provide a report on failed logins that supports monitoring of login attempts to its password safe and privileged activity record vault.
§164.308(a)(5)(ii)(D) Password Management (A)	Procedures for creating, changing and safeguarding passwords.	**Safeguard for Privileged Passwords** offers secure, full-featured, centralized management of privileged account passwords, including service account passwords. It can automatically generate passwords that meet an organization's password complexity requirements, set expiry times and dates for those passwords, and enforce password reset policy. In addition, requests for password changes are managed through a complete request review and approval workflow whose history is stored as securely as the passwords themselves: in a centralized password safe that is secured using full disk encryption.
§164.308(a)(6)(i) Security Incident Procedures		
§164.308(a)(6)(ii) Response and Reporting (R)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	With session recording, keystroke logging and access reporting on all privileged activity, **Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** help organizations identify, document and respond to suspected or known security incidents such as: • Anomalous user behavior, such as after-hours session activity • Potential breach incidents — for instance, access being requested and authorized to a system storing ePHI after business hours or during scheduled leave • Security policy violations like abuse of temporary elevated privileges during emergency break-fix situations

HIPAA standard and related implementation specifications		How One Identity PAM solutions help
§164.308(a)(7)(i) Contingency Plan		
§164.308(a)(7)(ii)(C) Emergency mode operation plan (R)	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.	In emergency situations, contingency plans can include paper-based or temporary electronic access to alternative sources of ePHI. Waiting for authorization to access these systems containing ePHI is often not practical, and pressure to share user accounts and passwords can be high. HIPAA compliance could suffer as a result. **Safeguard for Privileged Passwords** and **Safeguard for Privileged Sessions** can be used to develop procedures that support policies for accessing ePHI in the failover site access portion of an emergency mode operations plan to ensure ePHI access integrity (such as by eliminating the need to share passwords) for the continuation of critical business processes after a crisis situation to protect the availability and security of ePHI. In addition, these tools provide capabilities to perform periodic testing of emergency ePHI access procedures.
§164.308(a)(7)(ii)(D) Testing and revision procedures (A)	Implement procedures for periodic testing and revision of contingency plans.	
§164.308(a)(8) Evaluation (R)		
§164.308(a)(8) Evaluation (R)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity’s or business associate’s security policies and procedures meet the requirements of this subpart.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** can all reduce the level of effort required for periodic reviews of access authorization privileges (who can grant access to what) and privileged access management settings (who has privileged access to what) during required technical and nontechnical evaluations.

Physical safeguards

HIPAA standard and related implementation specifications		How One Identity PAM solutions help
§164.310(b) Workstation Use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	By imposing a variety of system and data access restrictions on users who are granted privileged access, **Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** all support the implementation of HIPAA-compliant policies and procedures for workstations that can access ePHI. The solutions can prevent a wide variety of suspicious activity and violations of workstation use policies, such as: • An employee account accessing systems after hours • An employee account accessing systems while on vacation or absent from work • An employee account accessing systems or data not appropriate for the employee's job • An employee account accessing high-profile or VIP accounts inappropriately • An employee account inappropriately accessing a system that contains ePHI • An employee account accessing a system that contains ePHI after employment termination

Technical safeguards

HIPAA standard and related implementation specifications		How One Identity PAM solutions help
§164.312(a)(1) Access Control		
§164.312(a)(2)(i) Unique User Identification (R)	Assign a unique name and/or number for identifying and tracking user identity.	**Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** go beyond native platform account management by associating specific users to shared privileged accounts with access to ePHI systems, thereby enabling organizations to identify who accessed which shared account at what time and what they did.
§164.312(a)(2)(ii) Emergency Access Procedure (R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	While not supporting ePHI access within EMR/EHR systems, **Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** are designed to help organizations manage access to privileged systems and environments (that is, those containing ePHI) beyond third-party ePHI systems (EMRs and EHRs). Often in emergency situations, waiting for required access authorizations to systems containing ePHI is not practical. Compliance with HIPAA could suffer as a result. By setting up an alternate authorization workflow, One Identity Privileged Management solutions can be used by organizations to implement appropriate emergency access to support systems and underlying platforms that store, protect or transmit ePHI.

HIPAA standard and related implementation specifications		How One Identity PAM solutions help
§164.312(a)(2)(iii) Automatic Logoff (A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	**One Identity Safeguard for Privileged Sessions** can limit access to systems containing ePHI to a specific session or period of time. It also enables administrators to terminate any active session, and records the termination event to demonstrate that the organization is complying with this requirement.
§164.312(b) 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.	With their activity tracking features, **Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** can provide audit teams with timed, recorded, scope-bounded, read-only privileges to privileged activities in virtually all information systems that contain or provide access to ePHI. Privileged activities can be audited by user and by system.
§164.312(d) Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	While still widely used in the industry, traditional user account/password combinations are fast becoming inadequate when used as the sole means of authenticating users who access ePHI. To meet the current standard of "reasonable and appropriate," organizations should consider implementing additional authentication safeguards in validating a user's identity, especially for users requesting access to systems storing or accessing ePHI. Options include access approval procedures and robust authentication controls such as strong passwords and mutual or multi-factor authentication. **Safeguard for Privileged Passwords, Safeguard for Privileged Sessions** and **Privilege Manager for Sudo** enforce a number of additional authentication safeguards, such as access approval workflows and the strategic use of temporary passwords that meet the requirements of strong password policies for ePHI systems. These solutions also supplement authentication validation controls by helping organizations identify or prevent common suspicious user account behavior such as: • An employee account accessing systems after hours • An employee account accessing systems while on the employee is on vacation or absent from work • An employee account accessing areas not appropriate for that employee's job • An employee account accessing high-profile or VIP accounts inappropriately • An employee account inappropriately accessing a system containing ePHI • An employee account accessing a system containing ePHI after employment termination • An employee account downloading known malware

Conclusion

The user access controls included in certified EHRs and other commercial ePHI applications provide only a portion of the security you need to achieve, maintain and demonstrate HIPAA compliance. You also need to manage privileged access to your organization's entire data environment — including all support systems and underlying platforms that store, protect or transmit ePHI.

Safeguard for Privileged Passwords, Safeguard for Privileged Sessions and Privilege Manager for Sudo fill this need, enabling your organization to substantially automate the enforcement of HIPAA standards for protecting ePHI in your broader ePHI environment. Plus, they deliver the automation you need to do so effectively and efficiently. For more information, visit oneidentity.com/solutions/privileged-access-management/

Joe Grettenberger has over 25 years of experience as an IT assurance professional, including eight years of technology auditing experience in both the public and private sectors. He is certified as an information systems auditor (CISA) and compliance & ethics professional (CCEP), and has served clients for over six years as an IT governance and risk management consultant covering a wide range of IT assurance issues within the regulatory, legal and industry compliance space.

Grettenberger has held IT audit, assurance and advisory positions at a number of organizations, including Modern Compliance Solutions, Quest Software, Vintela, Center 7, Franklin Covey and SAIC. He started his own consulting practice in 2008. He was a recent participant in the Internet Security Alliance initiative to promote cross-industry IT security standards, and he has also participated in several other standard-setting best practice initiatives, including serving on the SunTone Architecture Council and chairing the MSP Association's Best Practice Committee. compliancecollaborators.com

With One Identity Safeguard for Privileged Passwords, Safeguard for Privileged Sessions and Privilege Manager for Sudo, your organization can substantially automate the enforcement of HIPAA standards for protecting ePHI in your broader ePHI environment.

For More Information

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the license or sale of One Identity products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

About One Identity

One Identity helps organizations optimize identity and access management (IAM). Our combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, enables organizations to achieve their full potential – unimpeded by security, yet safeguarded against threats. For more information, visit oneidentity.com.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656