Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires significant changes in how the healthcare industry manages all aspects of information, including billing, reimbursement, security, and patient records. However, smart healthcare entities do not only achieve HIPAA compliance, they profit from it.

HIPAA provides opportunities to achieve efficiencies by automating key processes and eliminating manual functions. Healthcare organizations can gain a competitive advantage by moving from paper to electronic medical records—streamlining administrative costs and speeding claims payouts. However, most healthcare organizations still struggle to decipher the rules and meet the arduous requirements. HIPAA goes into effect in phases, allowing healthcare entities ample time to prepare for compliance with each of the rules. The initial phase is a legal burden for all covered entities—healthcare providers, hospitals, insurers, payers, and business associates (such as claims clearinghouses, billing companies, and others who enter into an agreement with one of these entities)—to comply with the HIPAA Privacy Rule.

Most likely your organization has already taken steps to safeguard patients’ health information under the new regulations. However, if your organization has not yet taken any action, it is critical that you start familiarizing yourself with HIPAA regulations. Assess the level of risk your organization can afford to assume and set your budget. Evaluate, test, and deploy those technologies that will help your organization attain and maintain its privacy and security goals.

This white paper examines how enterprise single sign-on (ESSO) creates a best practice for ensuring compliance with the Privacy Rule immediately upon implementation. ESSO can mitigate your organization’s privacy risk, save valuable time, reduce help desk costs, and improve security by authenticating medical professionals even in emergency situations.
What Is the Privacy Rule?

The HIPAA Privacy Rule creates national standards that set boundaries over the use and release of health information for protecting individuals’ medical records and other personal health data. Every time a patient sees a doctor, gets admitted to a hospital, goes to a pharmacist, or sends in a claim to a health plan, a record of the patient’s confidential health information is made. Before HIPAA, it was assumed that the doctor or the healthcare provider would keep the records sealed away in a filing cabinet.

HIPAA places a burden on healthcare providers to implement policies that protect against the misuse and disclosure of individual health information. Patients now have greater control over who has access to their information, while organizations must institute adequate safeguards established by the Privacy Rule to shield the privacy of their patients’ information. Civil and criminal penalties will be used to hold violators accountable for failing to guard their patients’ privacy rights.

HIPAA does not pre-empt the states from imposing further restrictions; it only sets certain federal minimum standards. This complex mix of federal and state laws will result in a bureaucratic maze (similar to the security industry’s blue-sky laws for regulating the sale of securities in each state). Not only will compliance be difficult, but it will also be extremely costly as the healthcare industry continues to computerize patient information and use the internet to access, research, and exchange medical data. On the positive side, remember this is your organization’s chance to simplify procedures, reduce administrative costs by cutting back on paper, and develop policies easy enough for all employees to understand and follow. As further inducement, your organization can lower its risk of suffering HIPAA penalties, negative publicity, lawsuits, and loss of accreditation.

Privacy and Security

**Privacy** refers to the right of individuals to control personal information and prevent its disclosure or use against their wishes. **Security** refers to the physical, technical, and administrative safeguards put in place to protect the integrity, accessibility, and confidentiality of information. The automation of patient health information (PHI) has escalated concerns of the government and healthcare industry about the security of computerized healthcare data. The growth in integrating electronic medical records, networking, internet access, and other technologies has not been matched by equivalent information security measures to secure data from unauthorized use. In 1997, the National Research Council reported pervasive weaknesses in healthcare security measures, such as user authentication, access controls, audit trails, controls of external communication links and access, physical security, systems backups, and disaster recovery.

Breaches of health information privacy, such as press disclosures of individuals’ HIV status, network hacking incidents, and misdirected patient e-mails, intensified the American public’s privacy concerns in the early 1990s. The healthcare industry and the Department of Health and Human Services realized that their HIPAA initiatives toward administrative simplification and automation would not succeed without requiring more-stringent information security measures. When HIPAA was passed in 1996, it included a mandate for standards that would ensure the security and integrity of health information stored or transmitted electronically. Organizations would be required to implement basic safeguards to
protect electronic protected health information from unauthorized access, alteration, deletion, or transmission. Therefore, ensuring privacy is interdependent with instituting appropriate security measures—although the HIPAA Security Rule is one of the last stages to go into effect.

Privacy Rule Impact on Healthcare Organizations

Healthcare entities must implement policies, procedures, and technologies that limit patient-protected information from being released without the patient’s knowledge and consent, beyond that required for patient care. Organizations are required to give patients a clear written explanation of how the entity can use and disclose their information. Audit logs must be maintained because patients have the right to discover how their information has been used and who has received their data. Patients have the right to examine and obtain a copy of their own health records, and request amendments. Patient consent will be necessary before healthcare providers can share information for treatment, payment, and healthcare operations.

In addition, separate patient authorization must be obtained for nonroutine disclosures and most nonhealthcare purposes. Patients have the right to restrict its use. In addition, a history of nonroutine disclosures must be available to patients.

Implementing technological solutions alone will not ensure the privacy of patient records, but the ability to control sensitive electronic information is essential to ensuring that only the minimum information necessary is exchanged between entities to achieve specific transactional ends. Therefore, healthcare providers, insurance companies, and anyone who handles medical information, such as benefits and payment transactions, need to ensure that all patient information is tracked and protected. Right now, although a breach in confidentiality could result in penalties, enforcement will primarily consist of waiting for formal complaints from patients. However, the media will be quick to publicize breaches of major public interest, which will lead to a loss of public confidence.

Therefore, HIPAA’s goal is to ensure that healthcare organizations use a reasonable standard of care as defined by HIPAA to protect patient health information.

A Reasonable Standard of Care

Doctors, hospitals, and other providers can continue to share patients’ medical information under HIPAA. HIPAA does dictate that the information shared is only on a “need to know” basis, and only the minimum amount of information necessary for authorized persons to perform their duties will be released to safeguard the information. To ascertain a reasonable standard of care, covered healthcare entities must assess the potential risks and vulnerabilities and take appropriate and reasonable measures to protect patient health information. More specifically, the healthcare organization must assess and define its needs, select and implement policies appropriate for its own environment, and use a risk assessment process that strikes a balance between risk and remediation costs. Its staff must receive adequate training and comply with these safeguards.

What happens if a prospective employer inadvertently gets a hold of a candidate’s health history? Perhaps the candidate submitted to a urine test, but the receptionist lets it slip that the candidate was treated for depression. A doctor writing an article for a medical journal might accidentally include data
that identifies patients. Pharmaceutical companies continue to purchase identifiable health data for marketing purposes. Hospital employees often use kiosks to quickly access PHI, but who locks the workstations down to prevent unauthorized people from obtaining patient data? Even the number of a celebrity’s plastic surgeries is private and protected under HIPAA. If a hospital’s staff member leaks the number to the press, the celebrity can take recourse against the hospital and doctor, assuming attorneys can trace it to the responsible party. All these risky events are subject to HIPAA regulations and cause for breach of privacy claims.

Data Protection Requirements

The Privacy Rule states that a legal health record consists of all individually identifiable data, in any medium, collected and directly used in documenting healthcare or health status that can be used to define the security responsibilities of a covered entity. Patient information must be securely guarded and carefully handled when conducting the business of healthcare. According to the American Health Information Management Association, an average of 150 people, “from nursing staff to x-ray technicians, to billing clerks,” view a patient’s personal medical records during the course of an average hospitalization. Under HIPAA, covered entities must implement the minimum necessary policies and procedures that limit how much protected patient information is used, disclosed, and requested for certain purposes. These policies and procedures must limit who in the organization has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business. The minimum necessary standard does not apply to disclosures made by healthcare providers for treatment purposes. By the same token, it does not exclude access to computerized medical information.

In a hospital setting, medical professionals should have to log on to and log off from workstations each time they use them to avoid the disclosure of information to unauthorized individuals, and thus ensure the integrity and accuracy of patient information. Doctors accessing patient should have to sign on and sign off workstations each time they use them to avoid the disclosure of information to unauthorized individuals and ensure the integrity and accuracy of patient information. Doctors accessing patient records from a laptop should have privileges that differ from the telecommuter-processing claims for a benefits provider. Each set of circumstances would be evaluated differently against the standards.

Properly implemented, ESSO maintains the security of countless applications, tracks and logs access of PHI, and speeds access to critical information. Passwords and other authentication methods are critical to meeting this minimum necessary standard to prevent the routine, unimpeded access of patient medical records by hospital employees when it isn’t necessary for the performance of their jobs. Unfortunately, one of the by-products of all this security is the multitude of passwords that healthcare staff and anyone else coming into contact with health records will need to remember to access all their applications, including diagnostic, clinical, and patient billing software. Security policies should designate standards for the password’s composition and frequency of change to avoid easily guessed passwords, and prohibit staff from sharing passwords (a common practice these days in most hospitals) or writing them on a sticky note by their workstations. Technologies should enable compliance, not hamper medical treatment.
Chain of Trust

Both the Privacy Rule and the Security Rule require covered entities to establish third-party agreements between themselves and all other entities with whom PHI is shared to protect the data exchanged. Specialists, claims clearinghouses, insurers, and billing companies are all third parties that must be informed and compliant with HIPAA. Patient information must be protected, even when it is no longer under the original party’s direct control. Periodic verification of compliance is essential. A designated official such as a chief privacy officer or chief security officer has to police compliance throughout the healthcare organization. Someone has to be held accountable for instituting appropriate safeguards and creating awareness among the workforce—doctors, nurses, orderlies, pharmacists, claims personnel, and volunteers.

Protect Patient Data Using Enterprise Single Sign-On

At a minimum, organizations are required to assess their potential risks and vulnerabilities and protect against unauthorized use or disclosure of patient data in their environment. A small practice might differ from a large health insurer in its privacy policies. The goal is always the same: to do everything reasonably possible under the circumstances to protect PHI. Healthcare organizations must prevent inappropriate use and sharing of PHI by medical professionals with legitimate access to the information. The real threat to privacy is the disclosure of confidential information to unauthorized parties by well-meaning or overworked staff. The recipients of such information requests will sometimes be unaware that the requests are illegal under HIPAA.

To control who accesses information, formal policies and procedures must be implemented that allow different levels of access to health information. No single policy, practice, or tool can ensure effective overall security. The safeguards that comprise HIPAA-mandated security focus on protecting the data integrity, confidentiality, and availability of individually identifiable health information.

Most healthcare organizations have always been concerned with the privacy of their patients’ information. HIPAA regulates the ability of patients to actually protect their rights and enforces compliance, particularly in the digital age. One of the most effective technologies to institute and document compliance is ESSO.

Single sign-on (SSO) is a simple way to (1) tie together proper user authentication and application access and (2) enable proper privacy controls. One ID and password authenticates the user for all required applications, such as prescription orders and patient records. SSO eliminates the need for health practitioners to remember multiple passwords, while retaining a high level of security for each application. A doctor can access patient records, prescription information, and other medical data using one-time authentication.

SSO accelerates access, and the medical staff spends less time worrying about logon problems. If you are trying to save someone’s life, then you don’t want to be caught in a password snafu.

SSO makes it easy for every user to start every computerized PHI session with proper authentication. Medical professionals no longer need to leave terminals logged on all day with one user’s name and password; they can easily sign on themselves. When combined with tracking and reporting by the SSO
solution, an institution can confidently tie every PHI encounter back to a specific access event. The result is user-friendly security combined with verified privacy. Audit trails facilitate accountability for patient information usage.

SSO does not mean that all applications use the same password. Users often confuse SSO with password synchronization, an older method for distributing and synchronizing a main password to other systems. True SSO solutions enable users to have different passwords for every application, to store these passwords in a protected database, and to make them available to the users upon login. The ESSO solution will retrieve the password from the database upon receiving a request for access—the logon is transparent to the user.

Budget considerations often factor into security decisions. Biometrics, smartcards, and public key infrastructure (PKI) are more expensive and time-intensive security technologies to implement. ESSO does not preclude applying those technologies in the future. However, an effective ESSO solution can be installed rapidly at a reasonable cost to quickly meet the minimum standards that HIPAA mandates. The goal here is not only to protect your patient’s privacy, but also to substantiate your reasonable standard of care should a patient make a formal complaint.

Selecting an Effective Enterprise Single Sign-On Solution

In selecting the appropriate SSO solution for your environment, consider its flexibility in meeting your long-term needs. Technology evolves at the speed of light. To minimize costs, any solution selected should be scalable to accommodate your evolving infrastructure and long-term strong authentication goals. In testing ESSO solutions, evaluate the application coverage, support limitations, integration methodologies, and return on investment.

There are many questions to answer before selecting your solution.

- **Does your SSO solution support all forms of authentication, including passwords, smartcards, PKI, tokens, and biometrics?** Your ESSO must meet changing security demands. A multitude of authentication methods are necessary in an environment that requires high security levels. In a small doctor’s office, SSO might be all that is necessary to secure PHI. A large hospital group would require several authentication methods.

- **What are the integration requirements?** Host-integrated ESSO often requires significant predeployment work on the administrator’s part to integrate applications into a central server using scripting agents. Integration costs are high, deployment time is lengthy, and coverage is often limited. This can result in reduced logon. Client-side intelligence eliminates or reduces the burden of integration—decreasing deployment time and increasing application coverage.

- **Is the authentication activity logged?** You want the ability to produce audit reports to confirm proper authentication at all levels. For example, a record should exist of every authentication event, regardless of where or how the access is provided. Each staff member should log on and off for security reasons. The administrator could set a specific length of time for automatic logoff.
• **Can you choose the appropriate level of security without sacrificing user convenience?** A doctor at a large hospital should have different privileges from a remote worker processing health claims for an insurance company. Prescription orders should require a higher level of authentication than the coding of a patient’s group plan.

• **Does ESSO support your current security policies?** You do not want to have to rewrite existing policies. The ability to build on existing policies facilitates training staff on procedures that they must follow. Your organization’s chain of trust is widened by strong, policy-based authentication.

• **What is the ROI?** The length of time it takes for your organization to recoup its investment in an ESSO is determined by the solution’s cost, amount of integration necessary, time it takes to deploy, and the reduction in user support and help desk costs arising from fewer password resets. Organizations easily spend hundreds of dollars per user each year on password-related issues alone. The inconvenience to the professionals in performing their medical duties, which can range from the mundane to the most urgent, should also be considered.

**Conclusion**

Healthcare organizations cannot rely on only one security method. Without a silver bullet, multiple layers of security from best-of-breed solutions are necessary to protect the organization from privacy breaches. The best ESSO solution enables you to quickly deploy it, works virtually everywhere, requires no integration, and supports other authenticators—hardening your security. ESSO automates every password management task for the healthcare practitioner with a legitimate need to access PHI. SSO helps by

• Making it possible to implement appropriate authentication and related security policy

• Ensuring that an organization can confidently provide secure access to PHI

• Simplifying compliance for the user

Properly implemented, ESSO maintains the security of countless applications, tracks and logs access of PHI, and speeds access to critical information. It is an effective method of authorizing access to personal health data and resources, and holding medical staff accountable for their activities. By deploying an ESSO solution, an organization can substantiate that it has made a reasonable effort to protect patients’ privacy by ensuring secure and reliable access.