

Enterprise Single Sign-On and HIPAA: A Best Practice in the “Good Faith Effort” to Protect Patients’ Privacy

A Passlogix Whitepaper

The purpose of this whitepaper is to demonstrate how SSO is an effective method of authorizing access to personal health data and resources, and holding medical staff accountable for their activities.



Content Index

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Privacy and Health Organizations
- Single Sign-On ties together Proper User Authentication and Privacy Controls
- How to Select an Effective Single Sign-On Solution

Enterprise Single Sign-on and HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires significant changes in how the health care industry manages all aspects of information, including billing, reimbursement, security and patient records. However, smart health care entities don't merely seek to achieve HIPAA compliance, they profit from it. HIPAA provides opportunities to achieve efficiencies by automating key processes and eliminating manual functions. Health care organizations can gain a competitive advantage by moving from paper to electronic medical records – streamlining administrative costs and speeding claims payouts. However, most health care organizations still struggle to decipher the rules and meet the arduous requirements. HIPAA goes into effect in phases – allowing health care entities ample time to prepare for compliance with each of the Rules. The initial phase is a legal burden for all “covered entities” – health care providers, hospitals, insurers, payers, and business associates (i.e., claims clearinghouses, billing companies and others who enter into an agreement with one of these entities) to comply with the Privacy Rule.

Assuming your organization hasn't buried its head in the sand, steps have already been taken to safeguard patients' health information under the new regulations. If you hired a Chief Privacy Officer, ran a Gap Analysis, assessed your organization's weaknesses, created privacy and security policies and procedures, acquired mission critical technologies and trained your staff, then you won't be caught in the headlights of your patients' newly acquired right to see how their information is used and protected.

What if proactive measures haven't been taken yet? It's essential that you, as a member of your organization's privacy team, get cracking. How can your organization quickly ramp up to protect patients' privacy under HIPAA? Start familiarizing yourself with the 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 paper examines Enterprise Single Sign-On (SSO), a best practice for assuring compliance with the Privacy Rule immediately upon implementation. Discover how this technology can mitigate your organization's privacy risk, save valuable time, reduce help desk costs, and increase security by authenticating medical professionals easily even in emergency situations. Vital features will be reviewed - persuading any organization from a small doctor's office to a large health maintenance organization (HMO) to implement single sign-on as a first line of defense in protecting patients' privacy rights. We will begin with a basic review of the HIPAA requirements.

What is the Privacy Rule?

The Privacy Rule creates national standards that set boundaries over the use and release of health information for the purpose of protecting individuals' medical records and other personal health data. It delivers comprehensive Federal protection for the privacy of health information. 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 their confidential health information is made. Before HIPAA, it was assumed that the doctor or the health care provider would keep the records sealed away in a filing cabinet. HIPAA places a burden on health care 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 preempt 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 (I.e.: the Security Industry's Blue Sky Laws for regulating the sale of securities in each state.) Compliance will be not only difficult, but also extremely costly as the health care industry continues to computerize patient information and use the Internet to

Enterprise Single Sign-on and HIPAA

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 – Hand in Hand

Privacy refers to the right of the individual to control personal information and prevent its disclosure or use against his wishes. Security applies to the gamut of physical, technical and administrative safeguards put into place to protect the integrity, accessibility and confidentiality of information. The automation of patient health information (PHI) has escalated concerns of the government and health care industry about the security of computerized health care 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. Pervasive weaknesses in health care security measures such as user authentication, access controls, audit trails, controls of external communication links and access, physical security, systems back up, and disaster recovery were reported by the National Research Council in 1997.

Breaches of health information privacy, such as press disclosures of individuals' HIV status, network hacking incidents, and misdirected patient emails intensified the American public's privacy concerns in the early 1990s. The health care industry and 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, assuring privacy is interdependent with instituting appropriate security measures – although the Security Rule is one of the last stages to go into effect.

What Does the Privacy Rule Mean for Health Care Organizations?

Health care entities must implement policies, procedures and technologies that limit the release of patient protected information 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 may use and disclose their information. Audit logs need to be maintained, since 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 health care providers can share information for treatment, payment, and health care operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients have the right to restrict its use. In addition, a history of non-routine disclosures must be available to patients.

Implementing technological solutions alone will not assure 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 in order to achieve specific transactional ends. Therefore, health care 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, while a breach in confidentiality may 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 and/or an outcry.

Enterprise Single Sign-on and HIPAA

Therefore, HIPAA's goal is to ensure that health care organizations utilize not less than a reasonable standard of care as defined by HIPAA to protect patient health information.

What is A Reasonable Standard of Care?

Doctors, hospitals and other providers can continue to share patients' medical information under HIPAA. HIPAA does dictate that 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. In order to ascertain a reasonable standard of care, covered health care entities must assess the potential risks and vulnerabilities and take appropriate and reasonable measures to protect patient health information. More specifically, the health care 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 – who authorizes its release and for what 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/or doctor, assuming attorneys can trace it back to the responsible party. All these potentially risky events are subject to HIPAA regulations, and are cause for breach of privacy claims.

What Data Needs to Be Protected?

The Privacy Rule states a Legal Health Record (LHR) consists of all individually identifiable data, in any medium, collected and directly used in and/or documenting health care 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 health care. According to the American Health Information Management Association (AHIMA), 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 health care 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 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.

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 isn't necessary for the performance of their jobs. Unfortunately, one of the byproducts of all this security is the multitude of passwords that

Enterprise Single Sign-on and HIPAA

health care 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 like a birth date, and prohibit staff from sharing passwords (a common practice these days in most hospitals) or writing them on a post it note by their workstations. Technologies should enable compliance, not hamper medical treatment.

Who Links into Your Chain of Trust?

Both the Privacy and Security Rules require covered entities to establish third party agreements between themselves and all other entities with whom PHI is shared in order to protect the data exchanged. Specialists, claims clearinghouses, insurers and billing companies are all third parties that need to be informed and compliant of HIPAA. Patient information needs to 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 health care 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.

Why Implement 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 end goal is always the same – to do everything reasonably possible under the circumstances to protect PHI. Health care organizations have to 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.

In order 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 “data integrity, confidentiality and availability” of individually identifiable health information.

Most health care 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 easiest, fastest and most effective technologies to institute and document compliance is enterprise single sign-on.

Single sign on 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. Single sign-on 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.

Single sign-on accelerates access, and the medical staff spends less time worrying about login problems. If you're trying to save someone's life by determining what he is allergic to, you don't need to be caught in a password snafu.

Single sign-on 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

Enterprise Single Sign-on and HIPAA

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 simple to use security combined with verified privacy. Audit trails facilitate accountability for patient information usage.

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

Budget considerations often factor into security decisions. Biometrics, smart cards and public key infrastructure are more expensive and time-intensive security technologies to implement. Enterprise single sign on does not preclude applying those technologies in the future. However, an effective enterprise single sign-on product can be installed rapidly at a reasonable cost to quickly meet the minimum standards mandated by HIPAA. The goal here is not only to protect your patient's privacy, but also to substantiate your reasonable standard of care in the event of a patient's formal complaint.

How to Select an Effective Enterprise Single Sign-On Solution?

In selecting the appropriate single sign-on product 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 SSO products, evaluate the application coverage, support limitations, integration methodologies and the return on investment (ROI.)

There are many questions to answer before selecting your solution, including:

Does your single sign-on solution support all forms of authentication, including passwords, smart cards, public key infrastructure (PKI,) tokens and biometrics (fingerprint, voice, face, iris and signature recognition)? Your SSO should be able to meet your changing security demands. A multitude of authentication methods are necessary in an environment that requires high security levels. In a small doctor's office, single sign-on 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 SSO often requires significant pre-deployment 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 sign-on. 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 SSO support your current security policies? You do not want to have to rewrite existing policies. The ability

Enterprise Single Sign-on and HIPAA

to build on existing policies facilitates training staff on procedures they need to follow. Your organization's chain of trust is widened by strong, policy-based authentication.

What is your Return on Investment (ROI)? The length of time it takes for your organization to recoup its investment in a SSO 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 professional in performing his medical duties, which can range from the mundane to the most urgent, should also be considered.

Conclusion

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

- making it possible to implement appropriate authentication and related security policy,
- assuring that an organization can confidently provide secure access to PHI
- and simplifying compliance for the user.

Properly implemented, SSO 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 enterprise single sign-on solution, an organization can substantiate that it has made a reasonable effort to protect patients' privacy by ensuring secure and reliable access. Enterprise Single Sign-On - a good dose of preventative medicine to protect your patient's privacy.