HIPAA Compliance with Immutable Proof, Using Blockchain Technology & Biometric Multi-Factor Authentication

by: Paul S. Heirendt, Founder & CEO, BLOCK id

HIPAA Security & Patient Privacy

The HIPAA act states that all healthcare providers and "covered entities" are required to ensure the protection of patient privacy; in particular, personally identifiable health information. Federal fines and criminal penalties have been established in the legislation for the unauthorized exposure of personally identifiable health information.

According to the U.S. Department of Health & Human Services publication: **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement**

> *"A HIPAA covered entity may disclose PHI to law enforcement with the individual's signed HIPAA authorization."*

Healthcare providers can be compliant with the HIPAA requirements and have proof of that compliance using BLOCK id™'s unique combination of technologies: Blockchain Identity management, strong biometric multi-factor authentication and immutable records stored securely and privately in BLOCK id secured Blockchain records.

HIPAA regulations require patient authorization in order to use or disclose "any protected information unrelated to treatment, payment or health care operations." This applies to information in any form, including information that is "maintained or transmitted by computer."

The Healthcare Industry (PROVIDERS: Physicians, Nurses, Pharmacists, Medical Centers, Health Systems, Laboratories, PAYERS: Insurance Companies, Third Party Administrators and others) has become increasingly concerned with HIPAA compliance.

- Providers need access to information from a multitude of different devices - computers, mobile devices, and telephones.
- Providers need access to information from a multitude of different systems.
- Providers are extremely mobile and often need access to information from outside of the healthcare system's secure network.
- Providers routinely use the telephone for consultations, transcription of medical records, placing orders for tests, retrieving test results, submitting prescriptions, renewing prescriptions, and retrieving patient information.
- Providers routinely wear gloves, which eliminates the use of fingerprint or hand geometry technologies.
- Patients need access to their health records from a multitude of different devices – computers, mobile devices, and telephones.
- Patients need access to their health records from a multitude of different systems.
- Patients need the ability to remotely control the authorization of access to their health records by healthcare professionals, and others.
- Payers need access to health records from a multitude of different systems with proof of authorization by the Patient and in some cases the Provider.

The BLOCK id *Voice Signature Service* enables new, more advanced healthcare applications and solutions not currently available, such as:

- Unique Blockchain based self-sovereign Identity with a unique BLOCK id for providers, patients and payers.
- The replacement of numerous passwords/PINs for active physicians/caregivers, increasing convenience and minimizing the opportunity for lost or compromised passwords/PINs.
- Enhanced physician/patient communications in a cost effective way through secure Internet based and Interactive Voice Response based applications.
- Secure mobile and wireless access to personally identifiable health information for patients and health professionals.

The HIPAA act states that all healthcare providers are required to ensure the protection of patient privacy; in particular, personally identifiable health information. Federal fines have been established in the legislation for the unauthorized exposure of personally identifiable health information.

HIPAA also addresses another critical provision - portability of information and patient access. These portability and access requirements are a major challenge to healthcare providers due to the lack of standardization in healthcare systems. Many

healthcare organizations are realizing that their current policies and systems are not sufficient to deal with the depth and breadth of the statutory requirements that the HIPAA legislation mandates. **These portability and interoperability requirements will represent the majority of the IT expenditures to meet the requirements of the HIPAA legislation.**

Finding cost-effective solutions for HIPAA compliance is an important issue. HIPAA implementations need to protect existing investments in computers and networks, while minimizing the financial and productivity burden of HIPAA compliant systems and processes.

Proof of compliance is a perfect use case for Blockchain technology, having a defensible record without it is difficult at best.

At its basic level, security measures are designed to protect data that is either stored or transmitted across organizational boundaries. Many security technologies used today address one or both of these basic goals. Even the government views security as an enabler. **One main goal of the HIPAA security standard is to provide a technical framework for organizations to guarantee patient privacy**. However, another fundamental goal is to improve the efficiency and effectiveness of the entire health care system by standardizing electronic data interchange and, ultimately, driving cost savings. As such, security is one of several standards that fall under the aptly entitled "Administrative Simplification" section of HIPAA.

HIPAA security standards final rule in its current "vendor- and technology-neutral" format. Health care organizations need to decide how to view security in light of their corporate strategy. Will it be an obstacle that must be cleared to meet HIPAA security requirements? Or, will security be viewed as an enabler that helps increase physician/administrator productivity, improves physician/patient clinical experience and facilitates collaboration between multiple facilities by securely using public networks such as the Internet?

Authentication for HIPAA Compliance

The Internet and related technologies provide enormous benefits to physician practices and groups, as well as to other segments of the health care industry. However, those benefits will not be realized unless a framework is set that assures online trust among those communicating and transacting. This means knowing with certainty the identity, rights and privileges of those with whom we are transacting. And it means providing an infrastructure for sign-on and role-based access control, policy compliance, confidentiality and data integrity via encryption, and non-repudiation via digital signatures.

As hospitals and other health care organizations move vast amounts of information online, they face a serious challenge - to allow the appropriate staff to access this information quickly and easily, while ensuring it does not fall into the wrong hands. While click-and-care dramatically streamlines the care process with real-time access, it falls short in two important areas - convenience and security.

The problem is that entry to these new clinical systems and applications is largely governed by passwords, which are not only easy to steal and break into, but also expensive to maintain. In fact, industry studies indicate that resetting compromised or forgotten passwords can cost up to $340 per user per year. Also, passwords are burdensome for caregivers to remember and use.

For example, a typical IS department may require doctors and nurses to use an eight-digit password that includes letters, numbers and different punctuation to access applications. How does the hospital staff respond**? They write the password down and stick it on the outside of their terminals, under keyboards or stick notes on their lab coat sleeves, sacrificing security for convenience.** Bottom line, in an environment that requires protection of patient information while making information readily available to physicians and staff, passwords just don't cut it.

Identity and Authentication

Trusted digital identity is required for authentication.

A BLOCK id is a Guaranteed Globally Unique ID (GGUID) for an individual, organization, digital or physical item, a set of digital or physical items, transaction, contract, account, interaction or a process step or state. A BLOCK id enables trusted retrievable blockchain records that are secure, scalable and blockchain agnostic.

When others have access to your sensitive information you are at risk as we have seen with the large scale breeches of "trusted" organizations.

BLOCK id enables the security of digital identity, rights management and privacy in the cloud using blockchain & multi factor authentication.

BLOCK id provides trusted identities for individuals, organizations, contracts, content and transactions that protect against identity theft, identity fraud, data manipulation and unauthorized disclosure of personal information.

Blockchain for Identity

KPMG in a report entitled **Demystifying Blockchain for Life Sciences**:

> *"Blockchain is a distributed ledger technology where transactions are recorded and stored with incomparable security."*
>
> *"Life Sciences is facing an unprecedented amount of data stemming from wearable, electronic health records and patient claims data. Pending regulations such as General Data Protection Regulation (GDPR) will only increase the focus on data privacy. Further, the final phase of the Drug Supply Chain Security Act (DSCSA) mandates interoperable exchange of serialized product data across all supply chain participants by 2023. We believe that Blockchain could be a key to interoperability and privacy."*

A quote from **Reconciling Privacy and Internet Freedom with Blockchain** by Alice Bonasio

> *"… the information is encrypted and can easily be secured by biometric identification, meaning that only you would ever be able to access and share it."*

Philip Rosedale Founder of Second Life

> *"I think that Blockchain is super important for money, for digital assets, **and most importantly for identity**. Not just in the virtual world, but in the real world. It stores that information in a way that only the owner who has the private key can be associated with that little chunk of the Blockchain. The owner can update the object, sell it, move it around. No company or central organization is able to do that once it's printed in the Blockchain,"*

Multi-Factor Authentication

Multi-factor authentication is recommended in order to meet HIPAA compliance, as it adds an extra layer of security that can prevent unauthorized access.

Authentication is a process that starts with the **Assertion** of an identity claim, the **Validation** of that identity claim and the **Authentication** of the individual asserting the claim.

An article from ModernHealthcare.com demonstrates the need for strong authentication in the healthcare industry. The Privacy and Security Tiger Team of the Health IT Policy Committee is proposing rules for Stage 2 meaningful use that will govern security recommendations to authenticate the identity of patients as they log into their patient portals to download or view their personal health records.

Most web and mobile login methods do not provide true "multi-factor" authentication; they simply use multiple instances of one factor (i.e., knowledge factors such as username, password, "security" questions, etc.). Such knowledge factors can be readily obtained by phishing attacks, key-logging malware, social engineering of live agents, "friendly/workplace fraud", "family fraud", etc. The stronger the password, the more likely that the user has to write it down to remember it.

Biometrics in Healthcare

Healthcare organizations are looking to Biometrics to provide the most secure, uniquely identifiable end-user authentication, while providing the most convenience for patients and staff. Biometrics is the process of taking uniquely identifiable data about a person and using this data to verify their identity. Biometric technologies include: fingerprints, hand geometry, facial recognition, iris scans, voice authentication, etc. Biometrics are nearly impossible to falsify, unlike other methods of authentication (passwords, PINs, etc.).

Capital Coast Health (CCH), a major health authority in Wellington, New Zealand, surveyed all users who requested a password change from the help desk to determine the level of password misuse. They found that users admitted to a moderate level of password sharing, to some difficulty in thinking of new passwords and, in some cases, to an amazing inability to recall passwords. About 5% of users reported in excess of six password resets in the previous six months. As the on-site Security Analyst commented, "Doctors can remember the name of every single nerve in the human body, but simply cannot recall a simple password!"

According to an article in Sm@rtPartner magazine:

> *"Moreover, government regulations soon may make biometrics virtually mandatory for health-care, financial and e-commerce applications."*

Novell, in their HIPAA implementation documents, states:

> *"Of itself, HIPAA does not mandate biometrics. However, many implementers are rapidly coming to the conclusion that biometrics are the simplest and most elegant method of implementing the levels of authentication and security required by this legislation."*

BLOCK id's *Voice Signature Service* (VSS) enables true biometric multi-factor authentication and immutable Blockchain records in web and mobile applications that is uniquely both convenient and secure with proof of compliance.

BLOCK id's VSS goes beyond the basic authentication function and provides the additional functions required by healthcare and the other market sectors BLOCK id serves. The "signature" model of the VSS, with its built-in compliance mechanisms and ability to recall/replay the actual speech utterances (Blockchain audit trail), allows Voice Signatures to meet the American Bar Association's requirements for a legally binding signature.

Function	Definition	Benefit
AUTHENTICATION	Assurance that the person interacting with the system is who they claim to be	The identity of a remote participant is confirmed in a user-friendly manner
AUTHORIZATION	The system only works when users cooperatively interact with the *VSS*	The cooperative act of a *VSS* user is analogous to the user signing a document or a credit card slip with their hand-written signature providing authorization.
AUDIT TRAIL	Each instance of a *Voice Signature* is securely stored and linked to the transaction by the use of a BLOCK id – stored in the Blockchain.	Ability to show that the authorization originated from an identified source, and provide immutable audit trails for proof in case of repudiation or to prove compliance.

The *Voice Signature* interaction is extremely convenient as it takes less than 9 seconds.

With BLOCK id VSS biometric multi-factor login, there is nothing to remember or lose. Voice Signatures are easily obtained by: an outbound call to the person's telephone number on file; a call to a toll-free number with an "extension" number; in an IVR interaction, in a call with a call center agent, or in an iOS or Android mobile app.

Once a person is enrolled in the BLOCK id d VSS, each subsequent authentication interaction returns a *Normalized Detector Scale*® confidence score (0 – 100) that can be used, in conjunction with relevant business rules, to allow the log-in, or take further steps to ensure that only the authentic person is able to log in. Beyond normal login applications, the VSS can enable strongly authenticated access to Medical records recorded "provable" HIPAA compliance.

Each VSS interaction is given a unique BLOCK id and recorded in the Blockchain, which provides an immutable forensic audit trail record – for unprecedented accountability of the person logging in transaction or interaction.

Consumer research has demonstrated that consumers appreciate the convenience the *Voice Signature Service* and they intuitively understand that *Voice Signatures* are security and privacy protective. They appreciate companies that provide privacy protection. Thus, consumer acquisition and retention is greatly enhanced.

Since the BLOCK id *Voice Signature Service* is provided as Software as a Service, it minimizes capital expenditures, minimizes internal development resource requirements, and boosts the ROI resulting from cost savings and customer acquisition & retention. In these challenging economic times, the cost & ease of implementation advantages of the *Voice Signature Service* can provide a significant competitive advantage.

BLOCK id's *Voice Signature Service* is a powerful Web Service that provides ubiquitous, on-demand voice authentication and legally-binding *Voice Signatures* that are recorded in the Blockchain to provide an immutable record of the transaction. The VSS meets federal requirements for strong multi-factor authentication for financial, healthcare, and other high security authentication environments. VSS has been in use for more than a decade for legally-binding signatures and strong biometric authentication for health and life insurance, federal programs: USDA, CMS, IRS, DoD and other security and signature applications.

Healthcare & Health System Example Use Cases

Call Center Applications

Enable migration of additional Call Center CSR interactions to IVR or Internet

- Replace cost of expensive CSR minutes with less expensive minutes.
- Strong Voice Signature authentication assures privacy and security of patient information.
- Streamlines and enhances the caller authentication experience.
  - Voice Signatures require no memory load
    - user is prompted with phrase to speak vs. remembering and entering different PIN#s, passwords, etc.
- Eliminates majority of cost associated with PIN# or password reset calls.

Streamline the caller authentication process for Call Center CSR interactions

- Reduce the CSR minutes associated with authenticating the caller's identity.
- Strong Voice Signature authentication assures privacy and security of caller information.
- Streamlines and enhances the caller authentication experience.
  - Voice Signatures require no memory load
    - user is prompted vs. remembering and entering different PIN#s, secrets, etc.
- Caller authentication can be automated at the front end of the call, or inserted at the time of a specific transaction or interaction.

Enables a unified authentication experience across disparate call center, IVR and Internet platforms

- Provides a consistent user experience across all Health System touch points.
  - Voice Signatures require no memory load
    - versus remembering and entering different PIN#s, passwords, etc.
- Simple, inexpensive API integrations provide a quick, affordable unification solution.
- Provides strong HIPAA compliance mechanism, potentially relaxing platform integration timeframes.

Reduced risk and compliance costs associated with HIPAA regulations

- Reduced risk from the compromise of private health information by external or internal parties [fines, negative publicity, loss of patient, physician and health plan goodwill].
- Cost avoidance via streamlining of HIPAA compliance mechanisms.
  - Simplified processes are enabled by the use of biometric, Voice Signature authentication that provides an electronic signature with an audit trail.
  - Reduced paperwork, record filing and storage costs, etc.

Network Access Applications

Enable migration of additional constituent interactions to the Internet

- Interactions with patients, physicians, pharmacists and employees.
- Strong Voice Signature authentication assures privacy and security of
  - Private health information
  - Proprietary content accessible on the Health System Web site.
- Consistent authentication experience with Call Center and IVR platforms.

Simpler, less expensive authentication of the actual user

- Eliminates the vendor cost and administrative overhead associated with digital certificates, "SecureID" tokens, etc.
- Eliminates the cost of existing password and PIN# reset applications, etc.
  - Voice Signatures require no memory load
    - user is prompted with phrase to speak vs. remembering and entering different PIN#s, passwords, etc.
- Voice Signature authentication can be associated with specific user "transactions" and provide the benefit of a legally binding signature (e.g., prescription orders, prescription refill requests, patient health history access, etc.).
  - Voice Signatures can be used for remote signing of documents
    - A digital digest of the document can be permanently stored in a BLOCK id Blockchain record with the Voice Signature record included, which "locks" the document with a Voice Signature and provides an immutable record.

Reduced risk and compliance costs associated with HIPAA regulations

- Reduced risk from the compromise of private health information by external or internal parties [fines, negative publicity, loss of patient, physician and health plan goodwill].
- Cost avoidance via streamlining of HIPAA compliance mechanisms.
  - Simplified processes are enabled by the use of biometric, Voice Signature authentication that provides an electronic signature with an audit trail
  - Reduced paperwork, record filing and storage costs, etc.
- BLOCK id Blockchain immutable record of compliance.

Other Applications

- Remote / electronic document signature applications
- Patient registration documents
- Facilitates electronic prescribing
- Requisitions
- Lab and other diagnostic or treatment orders
- Operative notes, medical record entries, etc.
- Forensic evidence collection and tracking

Conclusion

The HIPAA act states that all healthcare providers and anyone else in contact with or handling PHI (covered entities) are required to ensure the protection of patient privacy; in particular, the personally identifiable health information. Federal fines and criminal penalties have been established in the legislation for the unauthorized exposure of personally identifiable health information.

Covered entities can be compliant with the HIPAA requirements and have proof of that compliance using BLOCK id's unique combination of technologies: Blockchain Identity management, strong biometric multi-factor authentication and immutable records stored securely and privately in BLOCK id secured Blockchain records.