Healthcare Solutions Made Simple: Balancing Security and Convenience in Healthcare

Authored by Axiad IDS, HID Global, NetIQ

February 2017
Table of Contents

1. Introduction: Fundamentals of Data Protection in the Healthcare Industry . . . 1

2. Implications of HIPAA for Personnel Authentication ................................. 1
   Usability and user adoption........................................................................ 1
   Costs incurred, costs avoided............................................................... 2
   Security mandates................................................................................. 2

3. Planning Priorities .................................................................................... 2

4. Use Cases .................................................................................................. 3
   From simple authentication to SSO (single sign-on) to EMR (electronic medical
   record systems).................................................................................... 3
   Follow-me authentication (support in virtual desktop environments) ...... 3
   Tablets and mobile devices................................................................... 3
   Card roll-out: common concerns and scenarios ................................... 3
   Corporate/back office authentication...................................................... 4
   Temporary/partial workers................................................................. 4
   Electronic prescriptions..................................................................... 4

5. Simple, secure solution ............................................................................... 4
   Multi-factor authentication............................................................... 4
   Benefits of Axiad IDS’ bundled solution.......................................... 4

APPENDIX: INDIVIDUAL PRODUCT/TECHNOLOGY COMPONENTS OF AXIAD IDS’ SOLUTIONS

1. Authentication Software ........................................................................ 6
2. Credentials ............................................................................................... 7
3. Authentication devices/readers ............................................................... 9
4. Card Printers and Encoders ................................................................ 10
1. Introduction: Fundamentals of Data Protection in the Healthcare Industry

The information security demands of HIPAA are broad and cover everything from policy to physical and logical (IT) access controls. This white paper will address logical access controls to electronic records. There are three pieces of legislation that regulate or guide the protection of Personal Health Information (PHI):

1. **HIPAA**: The Health Insurance Portability and Accountability Act of 1996 defines standards, processes and responsibilities for covered entities* specific to data management and privacy. The security rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Source: hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

Transactions for which HHS has adopted standards.

2. **HITEC**: The Health Information Technology for Economic and Clinical Health Act of 2009 established a framework for the civil and criminal enforcement of HIPAA and defined categories of violations and associated penalties for Covered Entities.

3. **EPCS**: The Electronic Prescription of Controlled Substances rule from the Drug Enforcement Administration (DEA) aims to control the prescription and delivery of controlled drugs.

Although these three documents do not expressly dictate the technical means by which Personal Health Information must be secured, the documents provide guidance as to how Healthcare CISOs and CTOs must: 1) manage the access; 2) track changes; and 3) proactively react to changes or violations.

In practical terms, these three pieces of legislation have established the need to create several different but intertwined processes for the secure authentication, encryption, traceability and management of personal health information. In our opinion, the essential starting point to respond to HIPAA is to establish secure identities that cannot be easily ‘hacked.’ The industry has responded by offering myriad solutions generally falling under the category of multi-factor authentication (MFA) which are designed to thwart the inherent weakness of passwords.

Starting an MFA project either by itself or in conjunction with other adjacent solutions such as single sign-on and data encryption (at-rest or in-flight), requires healthcare organizations to take into consideration ROI, ease of use and ease of deployment.

2. Implications of HIPAA for Personnel Authentication

**Usability and user adoption**

Depending upon an organization’s specific configuration, any mix of personnel may come in contact with personal healthcare records (PHI) including: hired physicians and nurses, temporary or independent healthcare professionals, administrative staff, finance, contractors, and more. Implementing a one-size-fits-all solution does not work in this multi-faceted, ever-changing environment. For instance, a solution tuned to meet the needs of the finance department may provide sub-par speed and convenience for the tending physician, elevate administrative costs, or impose access limitations to external providers. Indeed, most healthcare organizations require a flexible, customizable solution to meet specific needs across various user populations.

Each technical solution for authentication has its pros and cons:

- **Biometrics**: Although these include face and voice recognition, only fingerprint readers/scanners tend to be cost-effective devices in a healthcare environment. Fingerprint biometric readers/scanners are easy to use, but present disadvantages of cost and possibly hygiene and health safety. In addition, these are highly technical devices that should not be chosen solely on price. A well-chosen reader/scanner must ensure the positive identification of a user each and every time, regardless of external factors such as dust, humidity, or dry/wet hands. Any organization planning to deploy biometrics should thoroughly test them prior to large scale deployment.

- **Contactless Cards and Fobs**: Many organizations issue employees contactless cards or fobs (common technologies include, Prox, iClass, DESfire and Mifare) to access facilities. In addition to opening doors, these contactless credentials can be leveraged for two-factor authentication. They present advantages in terms of cost, ease-of-use, speed and user familiarity. One downside of these contactless credentials is the inability to ensure devices, such as laptops or tablets, are locked once a user has finished a task and walks away. We view this as a small — but typically manageable — risk.

- **Contact Cards**: Contact cards, sometimes referred to as smart cards, used in conjunction with a certificates-based infrastructure — also known as Public Key Infrastructure (PKI) — provide the most secure solution commercially available. Combining cards and software similar to what is used by the Department of Defense, they give organizations an extensible solution for the long term, including: 1) support for EPCS; 2) document signature; and 3) email encryption.

The way these devices are used — requiring a card to be inserted into a reader and entering a PIN — provides both advantages and disadvantages. While smart cards allow...
organizations to enforce the locking of computer terminals at the end of a work session, they are sometimes disliked by physicians for four primary reasons: 1) they can be difficult to insert into a reader/scanner, especially when on a lanyard or reel; 2) concern with potential hygiene issues created by an open slot reader; 3) wait time to confirm authentication (typically less than 3 seconds); and the cost of implementation and administration of a smart card solution may be high.

**Costs incurred, costs avoided**

The costs involved in any solution will include:

- Direct purchasing costs of software and hardware
- Yearly support and maintenance fees
- Design and deployment costs (professional services and consulting)
- In-house staffing to manage the solutions
- Possible hidden costs such as help desk support, productivity loss when authenticating devices don’t work, time investment managing and supervising different vendors, etc.
- Direct fines, disclosure and remediation costs in case of a breach
- And perhaps, the costliest and longest-lasting impact of a breach: reputational damage

A rural/community hospital will likely look for a solution that is both cost effective and simple. A solution that avoids stitching software components from different vendors; leverages tested and certified hardware; and above everything else, provides one point of contact in case of escalation. A larger healthcare organization will also need to consider fit across multiple populations within the organization and/or across the enterprise. It is imperative that customers pick a software platform that enables as many different authentication methods and devices as possible to ensure all users and use cases have balanced security and convenience.

**Security mandates**

Healthcare organizations must implement a solution that can protect against breaches while not impeding day-to-day operations.

Two-factor authentication solutions, while not expressly mandated by HIPAA, are the de facto solution for elevating identity assurance. Indeed, they add a key layer of protection by replacing passwords (a very weak factor) with a combination of an external physical factor (something an individual owns or a personal characteristic) and something only the individual knows such as a PIN. Ultimately, the security of the solution depends on two separate elements: the technical element and the human element.

- Not all two-factor authentication solutions are equal in terms of security.
  - **Proximity cards** provide a reasonably good level of security that might be acceptable to organizations that are “small targets,” yet these cards can be reproduced easily.
  - **iCLASS cards** are a step-up from proximity cards and are a more secure technical option since they leverage symmetric encryption.
  - **PKI**, which leverages asymmetric encryption and “safe keys,” provides one of the highest levels of security commercially available.
  - **Biometrics** is in a special category: it is a solution that can be either extremely secure or weak depending on how it is rolled out. For example, biometric reader sensitivity can be increased or decreased, thus potentially opening the door to “false positives.”

- It is important to assess and plan for the way users will interact with a solution. If an organization can’t reign in and track the use of PINs and the sharing of cards by healthcare personnel, there is no reason to deploy a costly system.

**3. Planning Priorities**

1) A comprehensive strategy
2) Capacity to execute
3) Technology selection.

- **Strategy: best-of-breed or single-vendor solution?**
  There is no one-size-fits all solution. Healthcare organizations must find a partner that can complete a detailed use case analysis and technical assessment to define the best approach.

- **Capacity: hosted or in-house solution?**
  While healthcare organizations have grown increasingly comfortable with the idea of cloud-based IT solutions, leveraging the cloud in a data security scenario can still feel risky. The key is to carefully analyze pros such as speed of deployment, low maintenance/support costs, and one-time deployment, against the technical aspects of the hosted solution to ensure the highest levels of dependability and security.

- **Technology: physical and logical access convergence**
  Physical Access cards can easily be leveraged in what we call “convergence at the card.” While it is technically and organizationally challenging to have PACS (Physical Access Control Systems) and LACS (Logical Access Control Systems) truly converged from a system management point of view, simply leveraging a single credential to manage the physical and logical access is possible and does not disrupt the PACS already in place or the chain of command for access decisions at the IT and/or physical security level.
• **Deployment**
  Critical steps in managing an end-to-end deployment include:
  - Project management assistance
  - Workshop and documentation
  - High availability
  - Integration with existing or new systems such as single sign-on, printers, active directory, etc.
  - Accreditation and certification
  - Remote or on-site deployment
  - Training
  - Post-deployment assistance

• **Life after day one: support and long-term return on investment**
  Post-deployment support is perhaps one of the most critical aspects of a successful solution. Healthcare organizations should consider the following:
  - Too many parties involved in a solution without clear responsibilities and accountability can be a recipe for disaster.
  - Having a single-vendor approach can drastically limit choices or preclude customers from deploying the best solution.

It is essential customers engage a specialized solution provider that can demonstrate not only pre-sales savvy — but successful post-sales support and customer retention.

**4. Use Cases**

**From simple authentication to SSO (single sign-on) to EMR (electronic medical record systems)**

**Situation:** Secure authentication is mandated to log-in to Electronic Medical Record Systems (EMR) to protect patient data.

This is an important mandate for everyone but if you are a physician trying to save a person’s life, having to deal with the security requirements of this mandate can be quite frustrating when time is of the essence. As a result, healthcare organizations often resort to short cuts which can compromise security and ultimately harm patients.

**Challenge:** Healthcare professionals do not have time to log in to secure systems 20-plus times a day to simply access patient data and do their job.

**Solution:** By combining single-sign-on (SSO) authentication with a two-factor authentication solution based on smart cards, fobs, contactless bracelets or biometrics, healthcare personnel can log in and authenticate one time with the tap of a badge, providing seamless login to every application for the rest of the day.

**Follow-me authentication (support in virtual desktop environments)**

**Situation:** Nurses and physicians regularly use the same mobile workstations: the nurse checks the patient in and conducts the initial examination; the physician then arrives and conducts the official examination.

**Challenge:** The nurse must log in to the EMR to record the initial patient examination and then log out before passing the patient and workstation over to the physician. The physician must then log in to the EMR to record information about the same patient. If a change in examination areas is required the doctor must log out and then log in again in the new room or area. All of this is time consuming and outside of the healthcare professional’s area of expertise.

**Solution:** With a multi-factor authentication solution based on Linked Accounts or follow-me authentication, a physician can easily pick-up where a nurse left off. Similarly, if the physician needs to walk the patient to another room or area for additional tests, follow-me authentication allows the doctor to seamlessly pick-up from another secure device. Organizations using thin clients are best suited for this type of interaction.

**Tablets and mobile devices**

**Situation:** Physicians and nurses utilize a mix of tablets and mobile devices to access sensitive patient data. Access to the devices and the records in the EMR must be secured.

**Challenge:** Use of various mobile devices poses a challenge as it means securing multiple form factors. For example, a given environment may have a mix of iPads, Surface Pros and other mobile devices with USB ports. A practical solution for this scenario is necessary.

**Solution:** An acceptable solution could be based on small form factor biometric USB readers, an out-of-band authentication, or a notification-based authentication that allows users to authenticate with a touch of a button from their mobile device.

**Card roll-out: common concerns and scenarios**

**INITIAL ROLL-OUT**

**Situation:** Employees must be issued new cards and be re-badge when implementing a new secure authentication solution.

**Challenge:** HR departments believe it’s a logistical nightmare to issue new cards and re-badge their entire workforce when implementing a new solution.

**Solution:** With a customer self issuance portal, new cards can be sent to employees directly. For the logical access component, an email is sent to employees with a link to load their certificates.
STOLEN/LOST CARDS

Situation: A physician or nurse can’t access their workstation because they’ve lost their card and/or its been stolen.

Challenge: Time is of the essence in a medical situation. A second lost trying to regain access to a workstation could mean a life lost.

Solution: A centrally managed card system immediately deactivates lost or stolen user credentials so an intruder or hacker can’t access Protected Health Information. Physicians and nurses can then access workstations using an emergency password login set up by the IT Security team.

Corporate/back office authentication

Situation: Employees have a physical badge to access their building. Employees also need to have multi-factor authentication with a one-time password hard token to access applications on their workstation.

Challenge: Juggling multiple badges and access devices can be cumbersome and challenging.

Solution: With a converged access solution, employees can use their physical badge instead of an OTP to fulfill multi-factor authentication in accessing applications.

Temporary/partial workers

Situation: Companies hire contract workers and need to provide them access to sensitive company information for them to perform their work.

Challenge: It can be a challenge providing contract workers access only to the data they need and a hazard when contractors aren’t disabled from access at the end of a project.

Solution: With user profiles and card management systems, healthcare organizations are able to limit contract workers data access and disable access completely once they are no longer with the company.

Electronic prescriptions

Situation: To meet the DEA rule for EPCS (electronic prescribing of controlled substances), physicians and pharmacists need two-factor authentication to access applications allowing them to prescribe and deliver controlled substances.

Challenges: There are several considerations that must be taken into account to effectively comply with EPCS such as:

• Technical: While the traditional multi-factor authentication methods we’ve discussed in this paper — cards, tokens and biometrics — are valid options, there are technical restrictions in terms of the choice of access devices. For example, biometric readers and smart cards must meet FIPS-201 Personal Identity Verification (PIV) requirements. Only FIPS 140-2 certified credentials are compliant for EPCS which limits the options for a DEA certified solution. These credentials should be issued only after the prescriber’s identity has been vetted to LOA3.

• Usability: Healthcare organizations typically have an overlap in terms of the population who must comply with HIPAA and EPCS.

Solution: It is wise to implement a solution that doesn’t require additional devices or variations in user training.

5. Simple, secure solution

Axiad IDS’ MFA solutions make it easy for physicians to quickly access confidential information without compromising patient care. Powered by NetIQ’s proven authentication and single sign-on, and by HID Global cards, readers, biometrics and credential printers, with a single tap physicians get fast sign-on times. The same card gets medical staff in and out of cloud apps, Windows, and doors. Follow-me login enabled by virtualization technologies allows authorized personnel to move between workstations quickly and efficiently. Each minute saved means more time for patients and less frustration for staff.

Multi-factor authentication

Axiad IDS’ MFA solutions help healthcare organizations cost-effectively decrease the risk of breach by adding an extra layer of security now mandated by the U.S. government. Axiad IDS also provides 24/7 support for the complete solution — one software solution; one point of contact.

Benefits of Axiad IDS’ bundled solution

• Reduces risk of breach
• Addresses compliance needs
• Remove password vulnerability
• Provides a positive user experience
Appendix: Individual Product/Technology Components of Axiad IDS’ Solutions
1. Authentication Software

NetIQ Advanced Authentication to strengthen primary authentication

PRODUCT OVERVIEW

Multi-factor authentication (MFA) is one of the most effective ways to keep interactions secure as it provides secure access for customers, contractors and employees. User names and passwords are not enough to defend against breach; multi-factor methods are stronger and enable quick and accurate identification. However, authentication requirements are seldom the same for everyone or every scenario — the method must fit the user’s role and the situation.

NetIQ Advanced Authentication’s flexibility enables the authentication experience to be tailored at the level of protection required, and takes into account that not everyone needs the newest or most expensive appliance. Often, the badge used for building access can also serve the basic access needs of diverse populations across the enterprise. NetIQ Advanced Authentication lets organizations use as many different devices as they desire — or continue to use old ones while phasing in the new — under the same management and control.

It may be that not every secure interaction incurs the same level of risk for all types of users; rather, some interactions pose a greater risk to the organization. In these cases, organizations can use NetIQ Advanced Authentication to configure multiple authentication policies that invoke different procedures based on the situation. A higher-risk interaction requires a stepping-up of the verification — for example, another piece of information (something the user knows), out-of-band verification or another gesture. All of which administrators can manage centrally with NetIQ.

NetIQ SecureLogin for single sign-on

PRODUCT OVERVIEW

As a market-leading single sign-on product, NetIQ SecureLogin allows users to access local and network resources using a single set of credentials. When users log-in to a desktop, NetIQ SecureLogin automatically authenticates.
them to all of their applications and resources. Users only need to remember one password (or PIN, if combined with NetIQ Advanced Authentication) which obviates the need to write them down, create weak passwords because they are easier to remember, and call the help desk to reset a forgotten password. NetIQ SecureLogin virtually eliminates password-related calls to the help desk, enabling IT administrators to focus on new, value-added projects and end users to focus on their core duties.

- Organizations in healthcare and other high-security environments use NetIQ SecureLogin to integrate their smart cards, proximity cards and biometric devices with their applications and resources to create an optimal user experience that is both easy and fast.

- NetIQ SecureLogin enables organizations to strengthen their password policies. Users can be required to have more secure, or even randomly generated, passwords rather than those that are simply easy to remember. In addition, out-of-the-box integration and on-boarding technology allows organizations with smart cards, proximity cards and biometric devices to have it up and running in days, not weeks. NetIQ SecureLogin can also offer remote users password policy enforcement or an enhanced user experience for advanced authentication devices, whether the users are connected to the corporation’s authentication services or not.

- NetIQ SecureLogin does not require back-end servers or infrastructure additions, making it quicker and less expensive to deploy than competing solutions. Its broad, built-in support for applications and script-free integration wizard make connecting to applications a simple, automated process. This allows NetIQ SecureLogin to be deployed in a matter of hours.

- An intuitive interface simplifies installation and administration and provides integration with NetIQ’s other identity and access management products, such as NetIQ Identity Manager, NetIQ Access Manager™ and NetIQ Sentinel™. IT staff can centrally manage credentials and policies as well as monitor SSO activities. Administrators can easily grant application access by user or group and set preferences on what users may view and edit.

2. Credentials

NetIQ Advanced Authentication supports a broad range of authentication devices. The following are just a few examples of accepted devices:

**HID Global contactless cards**

Contactless cards are broadly used for building access or time and attendance. NetIQ Advanced Authentication allows use of the same card to protect access to end-user machines running Windows, Linux or Mac OS.

*Figure 2. HID contactless card with multiple technologies.*

Logging in to the machine can be as simple as tapping the contactless card on a reader attached to the machine. A PIN can be required to provide the second authentication factor, and may be cached for the day to improve convenience.

*Figure 3. Logging in by tapping the card on a contactless reader.*

**YubiKey**

A YubiKey is a small hardware device that offers two-factor authentication with a touch of a button. YubiKeys are strong enough for the largest enterprises, while remaining simple enough for anyone to use. The YubiKey NEO offers both contact (USB) and contactless (NFC, MIFARE) communications. YubiKeys support FIDO U2F, Yubico-OTP, OATH-OTP, OATH-HOTP, OATH-TOTP, OpenPGP, and PIV, and one security key can support an unlimited number of applications without the need for drivers or batteries.
HID Approve is a next-generation two-factor authentication solution from HID Global that delivers an exceptional user experience without compromising security. Through push notifications and a simple swipe-gesture, organizations can approve (or decline) an authentication or transaction request on a mobile device.

The same NetIQ smartphone app used for push notifications can also be used to generate a one-time password (OTP). This allows users to gain access to protected applications even if the mobile device is outside an area with coverage. The application can generate an OTP even when not connected to a mobile network carrier.

Generation of the OTP can be protected by an additional PIN configured within the application or simply leverage the mobile phone's security.

When generated, the OTP is displayed and valid for 30 seconds (this value is configurable, the OTP can be displayed for longer if desired). A progress bar clearly illustrates the time left for the current OTP.

The NetIQ Advanced Authentication smartphone app saves users time by letting them authenticate with a single tap of a button on their mobile device.

With NetIQ Advanced Authentication, a user's fingerprint can be used to authenticate to a machine. It also supports a broad range of readers: fingerprint readers that use Windows Biometric Framework (WBF), Lumidigm readers, and Digital Persona readers.

Fingerprints

With NetIQ Advanced Authentication, a user’s fingerprint can be used to authenticate to a machine. It also supports a broad range of readers: fingerprint readers that use Windows Biometric Framework (WBF), Lumidigm readers, and Digital Persona readers.

Figure 8. The Lumidigm fingerprint reader can read fingerprints through medical gloves.
PKI smart cards

PKI smart cards provide the highest level of logical security. These cards embed a microchip to secure digital certificates and perform the necessary cryptographic operations for secure authentication. PKI smart cards can be combined with contactless technology to secure both physical and logical access. The HID Crescendo Smart Card is the best example.

Figure 9. HID Crescendo card.

### 3. Authentication devices/readers

**HID Global card readers**

HID Global’s OMNIKEY readers are designed to support any smart card for any application on any computer. OMNIKEY readers support all relevant operating systems including Windows, Linux and Mac OS platforms. Certifications to all relevant industry standards including PC/SC, WHQL, USB CCID, EMV 2000, and Common Criteria ensure worldwide compliance and easy integration into any system.

Figure 10. OMNIKEY 5022 USB reader. One of many readers from HID that may be deployed depending on the specific use case.

**OMNIKEY 3021 smart card reader**

HID Global's OMNIKEY® 3021 USB is a high-performance smart card reader in a small form factor for desktop as well as mobile usage. It is an easy-to-install USB device suited for all contact smart card operations.

KEY FEATURES

- Small form factor
- Supports all major operating systems
- High-speed data transmission

Figure 12. OMNIKEY 3021 USB reader.
4. Card Printers and Encoders

FARGO® HDP5600 ID Card Printer and Encoder

It is critical to select the right printer for the application, including encoding and lamination. HID Global's FARGO HDP5600 ID Card Printer and Encoder is a high-resolution 600 dpi printing option for superior text and image quality. This all-in-one solution is ideal for healthcare facilities that need to routinely produce large volumes of high definition IDs or multi-function smart cards.

Organizations can print clear, crisp images, text and barcodes. Precise, complex characters such as Kanji, Arabic or Cyrillic are clearly defined and easy-to-read. The FARGO HDP5600 ID Card Printer and Encoder's 5th-generation re-transfer technology meets printing needs from sharp and vibrant photo ID cards to multi-functional, high security applications.

FEATURES

• High-quality resin printing for clear, crisp images, text and barcodes.

• Optional data encoding that produces highly-secure contact and contactless, multi-function smart cards to address specific needs and connect to other systems, such as visitor management, physical or logical access control, or time and attendance.

• Versatile, modular design with several field-upgradeable features that can be added as needs change. For example, an optional dual-sided, printing module can add company- or employee-specific information to the back of a card, such as when a bar code or digital signature is also desired. A dual-card hopper option simultaneously produces both employee and student or contractor IDs in a single pass.

• Cards, ribbons and over-laminate cartridges load quickly and easily, for easy operation and maintenance.

Figure 13. FARGO HDP5600 ID Card Printer and Encoder.