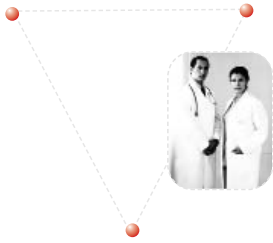




# HIPAA: THE CRITICAL ROLE OF STRONG AUTHENTICATION



The goal of this white paper is to highlight the aspect of HIPAA that pertains to patient privacy and authentication and the technologies that are available to assist in the achievement of HIPAA objectives.

*Author*  
**Jam Kahn**

**April 2002**

# CONTENTS

- OVERVIEW: THE GOAL OF HIPAA ----- 1
- HIPAA BENEFITS ----- 2
- AUTHENTICATION: A CRITICAL ASPECT----- 4
- SELECTING A COST-EFFECTIVE AUTHENTICATION MECHANISM----- 6
- BIOMETRICS ----- 7
- SMART CARDS----- 8
- USB KEYS ----- 9
- CONCLUSIONS ----- 10



## OVERVIEW: THE GOAL OF HIPAA

On August 21st, 1996 the Health Insurance Portability and Accountability Act became law. Prior to this, only voluntary standards were in place, which prevented the industry from moving to a single, efficient transaction environment. The goal of HIPAA is to reduce the cost and the administrative burden of health care by providing a specific standard, wherever possible, for electronic transmission of administrative and financial transactions. IT security infrastructures are being reviewed with the looming risk of fines and in severe cases criminal prosecution. The goal of this white paper is to highlight the aspect of HIPAA that pertains to patient privacy and authentication and the technologies that are available to assist in the achievement of HIPAA objectives.

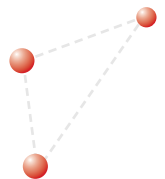
## HIPAA BENEFITS

For both health care institutions and patients, the HIPAA regulations represent a paradigm shift in the way we approach health care today. The Internet is an ideal medium by which HIPAA can achieve its goal. Whether helping patients to check medical records on-line or to have paperless prescriptions, there are several benefits that can be reaped by standardizing electronic transactions over the Internet. However, using such a medium means incurring increased risks as far as privacy and security are concerned. When used improperly, the Internet can be insecure, yet it is unparalleled in terms of cost and convenience and this is particularly appealing to health care providers.

There are strong laws that protect the confidentiality of patient records but, while these are necessary, they do not sufficiently address the issue of securing an individual's medical records. Clearly, such laws do not deter hackers. This is not sufficient to promote the growth of the Internet as a means of information gathering for patient records.

In a survey of CIOs from 100 hospitals, 93% of respondents listed HIPAA as one of the primary reasons for higher security budgets. Another 52% listed increased security threats, and 10% cited accreditation requirements. Some 21% of respondents acknowledged having a firewall breached while only 7% said their hospital was "very prepared" to ward off security breaches.

Security technologies currently in use at hospitals, according to survey respondents, include anti-virus software (100%), firewalls (96%), virtual private networks (83%), data encryption (65%), intrusion detection (60%), vulnerability assessment (57%), public key infrastructure (20%) and biometrics (10%). Virtually all respondents are expected to use all of these technologies to some degree during the next two years.



**The Secretary of Health and Human Services (HHS) is required to adopt HIPAA standards and among these standards are:**

- Unique identifiers for individuals, employers, health plans and health care providers for use in the health care system
- Security standards for health information
- Standards for procedures for the electronic transmission and authentication of signatures with respect to the transactions identified

Health information must be safeguarded both during transmission and while it is being stored. While the integrity of patient information is critical, the actual protection of individual patient records is of equal importance. This requires the ability to uniquely identify and authenticate an individual. With the right procedures and policies in place, the patient stands to benefit tremendously. Quality of health care would be affected dramatically. Patients today deal with multiple providers and being able to leverage a medium such as the Internet to access personal records can only have a positive affect. Administrative costs incurred by health care providers will be reduced as well. Indeed, few will deny the benefits that stand to be gained through HIPAA, rather it is the implementation challenge that has IT directors wary.

## AUTHENTICATION: A CRITICAL ASPECT

There are several security requirements for HIPAA privacy. These include:

- Authorization – enabling role-based authorization
- Authentication – unique identity assurance
- Access control – the ability to manage accounts
- Auditability – the availability of records to periodic audits
- Physical security – ensuring client uniqueness at the workstation
- Secure communication – cross-network security

There are several facets to HIPAA and it will require the use of multiple technologies working in collaboration to successfully address them all. The focus of this paper is authentication, the ability to provide unique identification for individuals and to strongly authenticate them.

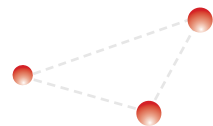
Authentication plays a critical role when it comes to security procedures. All security policies, encrypted sessions and secure data transmissions are of little value if the basic authentication scheme is weak.

Today health care records are protected based on a combination of a person's name, address, gender, SSN (social security number), phone number, health insurance number, birth date, employer and relationships to other family members. This use of personal information shows the glaring lack of privacy protection in place today, particularly if we take the example of HIV testing where individuals are assigned a unique number to assure anonymity. A similar approach should be taken to protect all transactions and medical records so that a person could not be matched based on their personal information.

Selecting this unique identifier is the challenge. The American Society for Testing Materials has published the Standard Guide for Properties of a Universal Health care Identifier (UHID), which provides 30 criteria against which candidate-identifiers must be gauged. There are six candidates that seem to come up the most frequently:

- Social security number
- Biometrics identifiers
- Directory service
- Personal immutable properties
- Patient identification system based on medical record number
- Public key cryptography

The scope of this paper is not to examine the UHID proposals, but rather to address the issue of the medium with which to use such an identifier. There are several choices with varying degrees of security. However, as often is the case, security and cost effectiveness have an inversely proportional relationship.



## SELECTING A COST-EFFECTIVE AUTHENTICATION MECHANISM

A hacker called "Kane" managed to download admission records for four thousand heart patients in June/July 2000 at the University of Washington Medical Center. (Security Focus, December 6, 2000).

Passwords are notoriously weak, albeit the easiest to deploy. Keep in mind that it is not the notion of a password itself that is flawed, but rather it is the type of passwords that are commonly used that lead to security breaches. Indeed all authentication schemes are ultimately passwords in a sense. Historically passwords have not worked because of the ease with which they can be hacked. One can make the claim that if a password can be memorized then it can also be hacked with relative ease. But as in any good security scheme, human limitations must be factored into the equation. The main goal of a hardware-based authentication scheme is to address this very issue. Biometrics, smart cards and keys seem to be the three most frequently discussed options in the hardware authentication arena.

## BIOMETRICS

Biometric solutions have the most appeal. They are not only secure but also give the user the sense of “high-tech” security that encourages acceptance. However, biometric solutions are not without their drawbacks. For one, the technology is still new and unproven. There is also the question of false positives and false negatives. No biometric device is 100% accurate so should valid users be occasionally disallowed (false negatives) or invalid users occasionally allowed (false positives)? Both cases could be argued for or against but more importantly both have drawbacks. No one wants to deny an authorized user, yet allowing access to an unauthorized user is equally unacceptable.

Another important factor that is often left out when discussing biometric solutions is that while a user is uniquely identified, most biometric solutions are still only one-factor authentication schemes. A fingerprint or retinal scan is nothing more than a large mathematical number derived from unique, immutable biological characteristics that make for a strong password. Yet it's subjected to the same replay-attack that a password is. If a hacker were to intercept this transmission and obtain this “password” it could be used in the future with malicious intent. While a biometric solution is a strong way to prove “who you are,” it does not address the “what you have” criteria that categorizes two-factor authentication.

In addition there is the stigma of biometric techniques being intrusive. By taking unique characteristics of individuals, it makes this technology seem somewhat big-brother-like in nature. In fact, it could be argued that even with biometric solutions a hardware key should still be used to ensure strong authentication and privacy.

But perhaps the biggest challenge facing biometrics is that of cost. As of now, biometric devices are not cost-effective. The technology is new and not widely deployed and so it's high-price-point stands to reason. But the ultimate goal of HIPAA is to reduce costs. If the cost of deployment is higher than the fines that are likely to be incurred, then motivation to be HIPAA-compliant is greatly reduced.

## SMART CARDS

Smart cards are an appealing choice. They are already widely deployed in European and Asian markets and have the familiar credit-card-like form factor with which we are comfortable. They are PIN protected making them very similar in nature to ATM cards that we use in our daily lives. Smart cards are typically associated with PKI deployments but this is not necessarily the case. As mentioned earlier, the nature of the UHID is not the scope of this paper, but certainly a smart card can be applied to most types of UHID's.

Yet smart cards have not seen the success in the United States that they have enjoyed overseas. And, for that matter, even internationally the PC market has yet to fully embrace smart cards. The reason: lack of a built-in reader. Applications and systems built specifically for smart card use (such as payphones) work extremely well. But for consumer acceptance in the PC market, a more convenient solution is required. Health care has often lagged when it comes to embracing new technologies. Smart card deployment would mean providing a smart card reader for numerous workstations including patients that wish to ensure on-line privacy. Aside from the foreseeable IT nightmares in achieving wide-spread smart card reader deployment there is also the cost involved. Smart cards are relatively inexpensive but the associated readers are not. Once again the goal of cost reduction is hindered.

## USB KEYS

Over the past few years the USB key has seen an increasing rise in user acceptance. Similar to smart cards in functionality, the USB key addresses three of the main smart card drawbacks:

- Lack of an ubiquitous reader
- Reader compatibility with PC's
- Cost of deployment

Virtually every PC in the market ships with a USB port today. This solves the problem of both having to deploy a reader and having to worry about compatibility issues. With the reader already built in, the workstation is already configured for use with a USB key. With interoperability being an important component of HIPAA, the USB key has a distinct advantage.

From a security standpoint USB keys are identical to readers. So much so that while some keys are merely a memory device others literally employ a smart card chip, making them interchangeable with compatible smart cards. Convenient enough to fit on a key ring, the USB key is user friendly and not intrusive. They are also more durable than smart cards, which are packaged in a thin plastic casing as opposed to the more rugged housing that a USB key provides.

Like smart cards, USB keys are flexible. Whether the goal is challenge-response-based authentication or PKI (public key infrastructure)-based, a USB key can be used.

At a price point that is about half the cost of a smart card and reader, the cost-effectiveness may be the USB key's most appealing characteristic. When balancing security versus cost with high-end biometrics at one end of the spectrum and passwords at the other end, the USB key is a secure, reasonably priced solution.

## CONCLUSION

HIPAA, while challenging and imposing, looks to dramatically improve health care as we know it today. For both the patients and the providers there is much to be gained. The patient will be able to leverage today's technology to ensure privacy and obtain access to medical records in ways that were unimaginable a few years ago. For the health care providers, their ability to provide exceptional health care while reducing administrative costs is greatly enhanced. Yet in spite of its many benefits, HIPAA compliance is not easy or cheap. There are several aspects that need to be considered and privacy is one that draws a lot of attention due to what is at stake. Doctor/patient privacy is nothing new and the Internet age cannot afford to compromise it. There is no single solution out there to address all the privacy requirements nor is there a standardized course of action to follow. HIPAA outlines guidelines and remains neutral when it comes to recommendations.

It is up to the responsible party to ensure that patient privacy and secure access is not compromised. Strong authentication needs to be employed and there are several options available. Efficiency, ease-of-use and costeffectiveness are the most critical factors in this arena. The bottom line, however, is that HIPAA advocates consumer-driven health care and any solution that's implemented should be made with the consumer in mind. ●