Why Healthcare IT Requires Strong Authentication

HillSouth

iT solutions.

Why does Healthcare IT Require Strong Authentication?

It's not only a good idea, it's **required** by HIPAA:

§164.312 A covered entity or business associate must…
(d) Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Of course, this could simply be with a user ID and password, but that wouldn't be enough for the real world. In the real world, you need to know for sure who logs in.

Identity assurance is even more important since the definition of a business associate has also been greatly expanded to include anyone handling or maintaining Protected Health Information (ePHI). Additionally, there's no distinction made between having access to and actually accessing ePHI.

Why: The Value of Information

Before we can look at why strong authentication matters, we need to remind ourselves what exactly is being protected.

In the case of ePHI, we're talking about records that potentially contain **every** piece of personal information about an individual, including their full name, date-of-birth, and even billing information.

Worse yet, in addition to the risks of identity fraud, some information is simply not suitable for public disclosure.

Doctor-patient confidentiality exists for a reason.

If a doctor's records or personal notes become public that information could potentially be used against the patient and/or the doctor.

Passing up on Passwords

It seems like every other week a new data breach hits the media, usually featuring some web service's personal and password data getting released onto the Internet with very flimsy protections on it.

Usually analysis of released data by security researchers show a large percentage of users are using passwords that simply aren't strong enough for **anything**.

Note: Many breaches become side-notes due to the frequency and size of the breaches that we do hear about.

Of course, it's entirely possible that some users will carry their poor password hygiene with them to work, even in healthcare.

The Human Condition

People are known for choosing passwords based on their family, pets, or random words related to their profession.

While a doctor could be using an extremely long word for their password like *Sesquipedalophobia* (the fear of long words) which will increase the level of protection from simply guessing random characters, an attack based off a dictionary of common words could still succeed.

If that password was the only protection for remote access to the doctor's workstation, that doctor now has a problem *he or she may not even know about.*

$e$quip3d@l0ph0bi@1: Not strong, but better than most.

Strong Authentication

Most users want simple systems. The average person will pick usability over security if given the choice. That's why successful IT service providers spend a significant amount of time studying the way their clients work before deciding how to implement strong authentication.

Lest weeks later, the service provider finds staff regularly circumventing the very systems intended to foster security.

The best implementations of strong authentication create a workflow that makes sense to the end users and doesn't slow them down.

Strong authentication doesn’t have to be disruptive.

It could be as simple as entering in a few numbers generated from a smartphone app or a key fob. Smart Cards and biometric scans can also count as a second factor of authentication. Speaking of which:

The Factors of Authentication

Something you know:	*A password, pin, etc.*
Something you have:	*A smartphone, keyfob, etc.*
Something you are:	*A fingerprint scan, iris scan, etc.*

Combine any two? *That’s two-factor authentication.*

House Calls

One advantage IT service providers have over doctors, is that IT people can usually work on their patients **remotely.**

Of course, if an IT service provider is repairing or upgrading a workstation that deals with ePHI they are considered exposed, *even if they don't actually access the ePHI*.

Thus, the same guidance that would apply to a physician remotely accessing a patient's file, applies to the technician who remotely works on that system. Which means *you* as the service provider need to be able to show **exactly** which technician accessed which machine.

This is where strong authentication can help with the record keeping. When using a proper strong authentication system, you can actually trust the system access logs. Plus, most systems will allow you to differentiate in the logs between users who have to perform tasks under shared accounts like "Administrator".

One thing to note: although the HIPAA Security Rule does not specify exactly what strong authentication is supposed to look like, we can turn to the federal government for some guidance. Check out OMB M-04-04 and NIST SP 800-63-1 for more details on what the government expects for those connecting to federal resources.

Also keep in mind, some of the resources doctors might access are considered federal systems, like the *Centers for Medicare and Medicaid Services*.

The Bottom Line

When someone accesses a resource belonging to a covered entity, there *must* be an appropriate level of assurance that the user is genuinely identifying themselves.

Not only is strong authentication very much required for Healthcare IT, it's a very good business practice to protect yourself, and even your clients who may not be in healthcare.

Ready for more?

With all the new and updated rules, it really makes sense to not only meet the standards, but exceed them where possible. That's where AuthAnvil comes in.

AuthAnvil is built from the ground-up for secure multi-factor authentication, in addition to secure password management and single sign-on.

Interested? Contact HillSouth about our HIPAA Protection plans and ongoing guidance and support with cloud based solutions such as AuthAnvil Multi Factor Authentication.

877.292.9070 or info@hillsouth.com

HillSouth

iT solutions.