Client Security

White Paper | June 2020

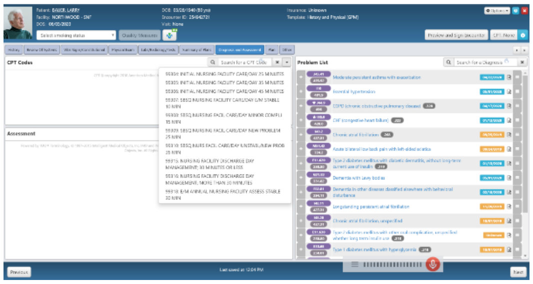
Purpose

Geriatric Practice Management (GPM) is often asked why the GEHRIMED™ application cannot be accessed directly through a web browser on end user devices. The purpose of this white paper is to document why GPM made a conscious decision to not allow web browser access to GEHRIMED.

Introduction

GEHRIMED is a complete ambulatory electronic health record created specifically for Long Term PostAcute Care (LTPAC) clinicians who face all the challenges of office-based clinicians, but without any administrative staff support. GEHRIMED was engineered specifically for clinicians providing direct patient care in the nation's 16,000+ nursing homes.

GEHRIMED is a fault-tolerant, cloud-based, Software as a Service (SaaS) application which is 100% paperless. The design incorporates an end-to-end HIPAA compliant security safeguard that prevents unintended Protected Health Information (PHI) exposure.



Patient: BAUER, LARRY
Facility: NORTHWOOD - SNF
DOS: 06/02/2020
DOB: 03/26/1940 (80 yrs)
Encounter ID: 254842721
Visit: None
Insurance: Unknown
Template: History and Physical (GPM)

99304: INITIAL NURSING FACILITY CARE/DAY 25 MINUTES
99305: INITIAL NURSING FACILITY CARE/DAY 35 MINUTES
99306: INITIAL NURSING FACILITY CARE/DAY 45 MINUTES
99307: SBSQ NURSING FACILITY CARE/DAY E/M STABLE 10 MIN
99308: SBSQ NURSING FACIL CARE/DAY MINOR COMPLI 15 MIN
99309: SBSQ NURSING FACIL CARE/DAY NEW PROBLEM 25 MIN
99310: SBSQ NURS FACIL CARE/DAY UNSTABL/NEW PROB 35 MIN
99315: NURSING FACILITY DISCHARGE DAY MANAGEMENT; 30 MINUTES OR LESS
99316: NURSING FACILITY DISCHARGE DAY MANAGEMENT; MORE THAN 30 MINUTES
99318: E/M ANNUAL NURSING FACILITY ASSESS STABLE 30 MIN

Moderate persistent asthma with exacerbation
Essential hypertension
COPD (chronic obstructive pulmonary disease)
CHF (congestive heart failure)
Chronic atrial fibrillation
Acute bilateral low back pain with left-sided sciatica
Type 2 diabetes mellitus with diabetic dermatitis, without long-term current use of insulin
Dementia with Lewy bodies
Dementia in other diseases classified elsewhere with behavioral disturbance
Longstanding persistent atrial fibrillation
Chronic atrial fibrillation, unspecified
Type 2 diabetes mellitus with other oral complication, unspecified whether long term insulin use
Type 1 diabetes mellitus with hyperglycemia

Last saved at 12:04 PM

Secure client access to the GEHRIMED application is integral to maintaining the security safeguards which ensure unintended PHI exposure. Unless GEHRIMED can maintain 100% confidence in the security of the end user access, the transactions conducted cannot be deemed PHI compliant. The end user method to access GEHRIMED is just as important as the security safeguards maintained and monitored in the GEHRIMED data centers.

The technical requirements for GEHRIMED do not list supported web browsers. This was intentional. Web browsers are notoriously insecure. GEHRIMED is only accessible from end devices via the GEHRIMED application on Windows, GEHRIMED iPad Application on iPads and the GEHRIMED application for MAC-based laptops and desktops.

Web Browser Insecurity

Web browsers are provided natively in the computers' operating system or created by a third party for free distribution. Internet Explorer, Edge, Chrome, Firefox, Opera and Safari are just a few of the available web browsers.

Web browsers are at heart a piece of software which requires constant updates and patches to correct bugs and provide new capabilities. Unlike most software, browsers must be able to communicate in a secure fashion with external internet sites. Browsers are, in effect, the most used software that allows end users' communication with the internet site. Anything from the latest weather to personal financial data can be accessed.

Web browsers, along with their underlying operation system, are some of the most attacked pieces of software. Outside entities look for vulnerabilities in web browsers to exploit for nefarious purposes. Malware is designed to exploit these vulnerabilities and capture data transmitted between the end user and the internet site.

Browsers also have a flaw with the way they function. Browsers store information from websites in both temporary files and cookies. These files are kept locally on the end user device. Those files can be accessed to compile information and reconstruct web sessions. Secure websites are designed to remove any critical data from those local files as the sessions are closed. But the possibility exists of a power issue, or even the web browser not deleting the file correctly, leaving critically sensitive information intact on the drive.

There are several methods to combat browser insecurities:

1. Encrypt drives on end user devices.
2. Update operating systems and web browsers with the latest patches.
3. Configure security in your browser settings:
    - Disable JavaScript.
    - Disable Java.
    - Use a pop-up blocker.
    - Don't cache your passwords or saved form information.
4. Update Adobe Flash software.
5. Remove administrative rights (enforce privilege authentication for software installation).
6. Install Anti-Spyware/Anti-Malware/Anti-Virus and keep up to date with current versions.
7. Think before you click!

Man-in-the-Middle (MITM) attacks

A MITM attack is exactly what it says. An attacker inserts themselves in the middle of a secure conversation between an end user and an internet service. The attacker intercepts messages from both parties, records them, and then forwards the intercepted messages to the other side. This type of attack can, but does not require, software installed on the local machine. Forms of MITM:

1. Man-in-the-Browser. Malware installed on the end user device which intercepts the traffic and can bypass encryption and anti-virus software.
2. Man-in-the-Mobile. Attackers use certificates to gain access and then intercept data from a free mobile app.
3. Man-in-the-Cloud. Attackers gain access by intercepting secure tokens and spy on transactions, file sharing and storage.
4. Man-in-the-Internet of Things (IoT). Devices that use Bluetooth or the internet (wireless security cameras, printers, biomedical devices, etc.) without default usernames or passwords.
5. Wi-Fi Eavesdropping. Hijacking a Wi-Fi connection, usually in a shared, public Wi-Fi setting.

The Department of Health and Human Service (HHS) Office for Civil Rights (OCR) have identified the MITM and HTTPS Inspection Products as key concerns for EHR. In their documentation they have described several high-level risks associated with MITM attacks and Secure Hyper Test Transport Protocol (HTTPS) inspection products. The details are very technical, but the advice given is to use certain types of Secure Socket Layer (SSL) certificates, Transport Layer Security (TLS) V1.2 or higher and ensure the HTTPS interception product properly validates certificate chains.

These recommendations must be implemented, along with proper security validation checks against the end user device web browsers, to ensure the integrity of secure transmissions.

GEHRIMED Client Security

When the GEHRIMED application was being developed, a conscious decision was made to only provide access to the cloud systems using a GEHRIMED client. That decision was based upon several factors, including:

- No control over end user devices. There are techniques where a website can check the end user system and not be allowed to run. But disabling a clinician from using GEHRIMED because a browser update was not installed was counterintuitive to the idea of always available access.
- Browser plug-ins have privileged access to the content of websites and should not be used in a HIPAA environment; without controlling the

browser itself GEHRIMED would not be able to prevent the use of insecure plug-ins.

- When a bug or new functionality is released the GEHRIMED client will force an update the next time a user logs in. This keeps the GEHRIMED client up to date with all patches, including any security enhancements.
- Proper HTTPS inspection methods. GEHRIMED controls all aspects of the secure end-to-end encrypted transmission, including the ability to detect when a MITM attack is attempted. GEHRIMED knows information about the SSL certificates used and can therefore understand when an improper formed encryption packet is received. This allows a far deeper inspection of the data to ensure the integrity of the underlying data.
- Ability to increase security as standards change. The GEHRIMED client and associated cloud systems are constantly updated with the latest security enhancements, such as SHA256, TLS V1.1 and V1.2, disable of all SSL versions and TLS V1.0 protocols, public key lengths increase from 2048 to 4096 bits, etc. GEHRIMED implements these security changes shortly after released and tested, forcing the updated security to be downloaded with the latest clients.
- One of the ways to ensure PHI confidentiality is to make sure no data is kept on the end user device. Web browsers cannot operate in this fashion. The GEHRIMED client creates a 'secure-bubble' where data is only kept in memory on the end user device. Data downloaded manually from the GEHRIMED client uses strong encryption to ensure protection.
- Strong OS integration: providing a native client for GEHRIMED allows us to provide secure access to local resources, which is how we can securely auto-import audio files (when requested) from digital audio devices connected to the user's machine. A browser limits access to system resources, preventing such seamless workflow.

Conclusion

The entire purpose for GEHRIMED is to allow LTPAC clinicians to document direct patient care – the definition of PHI. GPM has integrated security into the DNA of the company and the GEHRIMED application since its inception.

GPM weighed the ease for end users' access to GEHRIMED via web browsers vs. the HIPAA Security requirements and determined that there was too large a risk to allow web browser access to GEHRIMED. That would have been the easiest route to development, but not the route that would guarantee secure connectivity.