COVID-19 Client FAQ
HIPAA and Working Virtually

Updated March 24, 2020

We have received several questions regarding HIPAA compliance and virtual workers. At its core, HIPAA was designed to provide privacy standards to protect an individual's health and medical records as well as other health information.

Electronic health records store both personally identifiable information (PII) and protected health information (PHI), but they are just one component to enable HIPAA compliance. For example, the workstations provided by your IT department are a component to HIPAA compliance, as are policies around access to those devices. These are just two examples of items that are related to HIPAA compliance outside the core EHR, but there are several others. This document is intended to address some frequently asked questions and other topics to consider regarding remote workers and HIPAA compliance.

Do Netsmart applications have technical safeguards as required by HIPAA when my employees work virtually?

Our applications enable HIPAA compliance when accessed from an employee's home network. All Netsmart solutions ensure encryption and secure data transmission between the personal computer/workstation and backend system.

Clients are advised to review best practices with employees regarding screenshots and handling any data, such as printouts, at home in compliance with HIPAA.

Can my employees use their home personal computers to access my Netsmart solutions?

While your employees can likely access the solutions from their home personal computers (PC), it is NOT recommended for several reasons. You cannot guarantee the following or enforce policies on an employee's personal computer or virtual work environment:

- Anti-Virus/Malware software is in place
- VPN software
- Security updates installed
- Physical security of PC
- Password requirements to gain access to PC
- Screen lock policy
- Printing
- Data saved locally (i.e. control of data)

Note: Some hosted clients have Plexus network policies in place to only allow connectivity from their respective networks.

What are the differences connecting from an employee’s home network vs. my corporate network?

When connecting from your corporate network you have firewalls and other mechanisms to ensure secure connectivity to the internet (in addition to all the protections listed above). When connecting from an employee’s home network you cannot ensure a secure internet connection is in place, the performance of the home network, nor if there are other bad actors on the network.

What does Netsmart recommend for accessing solutions when working from home?

- Only access solutions from company-provided and managed devices
- Use a VPN software to connect to a corporate network
- Implement virtual desktop technologies such as Citrix. Netsmart can provide a virtual desktop solution for accessing your environment.

What if I have no choice but to allow my employees to use their home personal computers?

If there are no other options, it is STRONGLY recommended to only leverage a virtual desktop solution, like Citrix. Attackers look for a vulnerability to deliver their attack and will likely attempt new phishing attacks related to COVID-19. Without the security of a corporate network, VPN or secure virtual desktop like Citrix, risk is increased. When using Citrix, you control the desktop security and the internet connection from the Citrix server, creating a secure environment and connection as well as an optimized user experience.