Performing an OP Client-Server Risk Assessment

Last Modified on 09/18/2023 9:53 am EDT

It is important to perform a risk assessment on all EHR-related items configured on your office network since they access or store Protected Health Information (PHI) and are subject to HIPAA regulations. Performing standard, periodic risk assessments and audits on your network can help prevent or reduce the impact of a security incident. Anything that runs or works with the OP software could potentially manipulate or destroy confidential data. Every environment is unique, so we cannot provide a blanket step-by-step procedure for performing your own risk assessment. **It is up to you and your IT provider to determine the optimal security configuration for your specific environment.**

However, there are several general privacy and security safeguards that should be maintained within the OP software for a client-server environment:

- The OP software database must be password protected at all times. This includes the live production database and any backup files. It is the practice's responsibility to maintain the physical security of its hardware that runs the OP software and services. This includes hardware or software level encryption and secure storage of all PHI.
- The OP software does not store PHI in temp files, cookies, or other types of cached data on the end-user's local device when the EHR application is manually shut down under normal conditions. When the system is shut down manually, the OP software deletes the entire data cache during normal program termination. Because the OP software does not store any PHI locally on the end-user's device after the application is shut down, it is not necessary to encrypt this information. Abnormal program termination, such as from a power outage or software error, may result in orphaned files which do contain PHI. It may be necessary to manually remove these files.
- Reports and documents containing PHI can be printed or exported to a connected drive from the OP application via the main application or the database viewer. **These reports and print jobs are user generated**(e.g., a billing report or a PDF copy of the chart records). It is recommended that only people with the proper security knowledge be given access to the OP database viewer and that audits be performed periodically to locate any PHI on local or network drives.