On-Premises Information Security

Last Modified on 09/18/2023 11:16 am EDT

If you have an on-premise server, you should ensure that your server and user workstations are fully up to date with the latest security patches. In addition, it is important that your current anti-malware solution is fully up to date and running on all servers and workstations.

Basic On-Premise Practice Security Checklist

□ All servers running OP applications and services, as well as end user workstations, are running a currently supported operating system and are fully up to date with the latest security patches from the vendor.

□ You have deployed an anti--malware solution to all servers and end user workstations and it is fully up to date. Real time protection options should be active within your solution.

□ Your firewall is up to date with the latest stable firmware available and your firewall rules are in line with best practices related to OP application requirements and the healthcare industry.

□ Your on-premise server is fully backed up at least once per day and that you have a complete disaster recovery plan in place in the event a restoration is needed. You should work with your IT provider to develop a backup and recovery strategy that provides an appropriate recovery time objective (RTO) and recovery point objective (RPO).

□ Your on-premise server is located within a secure room that is only accessible by approved personnel.

Every environment is unique. These are the minimum recommended security practices and should only be considered a starting point. You should work with your IT provider to develop an information security and risk management plan that meets your specific needs.

If you have an on-premise server, and would like OP to keep your customer data secure by migrating to OP Cloud, contact your Account Manager for details.