ONCLOUD SECURITY SUMMARY

Server Security

1. OnCloud servers are protected by dedicated hardware and software firewalls.
2. Physical access to OnCloud servers is restricted and monitored 24/7.
3. OnCloud's hosting provider (Microsoft Azure) guarantees 99.95% uptime.
4. Azure Security Center with Qualys Agent used to monitor all OnCloud assets.
5. Azure Endpoint Protection Service applied to all resource groups.
6. Microsoft antivirus service and automatic security patches are employed and managed by Microsoft.
7. OnCloud maintains separate dedicated servers for production and development environments.
8. Server and web application security is tested and audited every month by security firm Qualys.

Password Security

1. OnCloud user sessions timeout in 5 minutes.
2. OnCloud requires strong password security.
3. Password lockout for multiple retry is employed.
4. OnCloud requires password change every 120 days.
5. OnCloud user status automatically set to "inactive" after 120 days with no login.
6. Brute force protection for SQL Server utilizing RDP Guard.
7. A detailed user login and transaction access log is maintained.

Data Security

1. 256-bit Secure Socket Layering (SSL) employed for all client-server transactions.
2. All Protected Healthcare Information (PHI), patient identifiers and file uploads are natively encrypted in SQL Server Enterprise Edition using Transparent Data Encryption (TDE).
3. Azure Disk Encryption is used to encrypt all virtual hard drives.
4. OnCloud users only have access to the hospitals to which they are assigned.
5. OnCloud data is backed up daily to a secure remotely using Microsoft's Geo-Redundant servers.
6. OnCloud system backup files are encrypted, password protected and tested quarterly.

HITECH / HIPPA

1. OnCloud users are required to participate in annual HIPPA/HITECH security training.
2. OnCloud subscribers must sign a Business Associate Agreement with Perfusion.com, Inc.
3. OnCloud subscribers are required to have HIPPA / HITECH policies in place.