



Designed for smaller hospitals, the OBIX Hosted Solution offers OBIX as a Service for obstetric units. The OBIX Hosted Solution delivers the features and functionality of the traditional OBIX Perinatal Data System via the cloud.

Migrating clinical applications to the cloud may seem daunting compared to the traditional premises based solutions, especially when it comes to the security of the data. For this reason, CCSI works with AWS to leverage their expertise and service reliability. Along with these pooled resources we have made sure that security controls are in place from our secure https webserver, firewalls, limited outbound and inbound rules, and isolated data locations.

OBIX Hosted Security Layers

The building blocks of security for the OBIX Hosted Solution have been established through its communication relationships. The first layer is through our partnership with AWS. The second layer is through CCSI security protocols around the OBIXCloud infrastructure and access to the OBIX software. The third and final layer is through hybrid cloud secure shell communication between the hospital WAN to the OBIXCloud in AWS.

AWS

Protecting data and information is as important to us as it is to our customers. To maintain standards through our certified Quality Management System, it was essential to select a proven leader for our first layer of security. Amazon offers one of the most secure web services in today's market. Their reputation and experience are trusted by many companies across various industries and the reason we make use of their datacenter and infrastructure for our OBIX Hosted Solution.

AWS offers multiple layers of security protection through credentialing, encryption, endpoints and multifactor authentication. In addition to their security measures, AWS supports healthcare compliance including certifications for several compliance programs such as HITRUST and others¹.

CCSI Security Protocols

CCSI implements additional measures on top of AWS procedures to ensure hospital data is stored securely providing the second layer of security protection. Unlike some other hosted software solutions, for each individual hospital we deploy an instance of the OBIX software and associated application servers in a dedicated container. Many other hosted software solutions deploy a single instance of software and each customer's database is then segmented. In this situation, although each customer's data is separate, the software itself is not isolated and is therefore more susceptible to corruption through multiple channels. Therefore, by installing the OBIX Hosted Solution in separate instances, should one database be breached, the other instances are isolated mitigating risk by a single occurrence.

Additionally, access to the hosted solution is restricted to key CCSI and hospital personnel to reduce breaches or inappropriate system use. CCSI has developed quality control and assurance standards that meet ISO, HITRUST, and SOC2 criteria.

Hybrid Secure Shell Communication

All required interconnect hardware, from cables to the OBIX Communicare (OC) Device and Moxa terminal servers is provided and included with the OBIX Hosted Solution. The OC device and Moxa terminal servers do not store any data

¹ <https://aws.amazon.com/health/healthcare-compliance/>
<https://aws.amazon.com/compliance/hipaa-compliance/>
https://d0.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf
<https://aws.amazon.com/health/providers-and-insurers/>

