Private. Really, Really Private.

OCI Software is committed to prioritizing and exceeding the highest standards of data security and availability for its AmbuPro Cloud customers. Recognizing the critical importance of safeguarding sensitive PHI & PII information and surpassing HIPAA standards, OCI Software has expertly designed and implemented the AmbuPro Cloud to be the most customer-centric and secure data hosting infrastructure possible.

Rather than utilizing a typical SaaS architecture where endpoints are publicly accessible (attack-prone) and customers are sharing resources in a multi-tenant environment (degradation-prone), the AmbuPro Cloud is a unique and 100% privatized approach. As such, each AmbuPro Cloud customer benefits from its own dedicated network, virtual server, and SQL Server instance, all of which are exclusively accessible by their trusted AmbuPro devices.

While this tailored infrastructure is the foundation of the AmbuPro Cloud, OCI Software has further implemented a comprehensive and robust zero-trust infrastructure to ensure enhanced confidentiality, integrity, and availability of data within the AmbuPro Cloud.

Key Security Principles & Practices.

Network Micro-Segmentation. Each customer on the AmbuPro Cloud operates within its own dedicated and private network that is strictly controlled, yet accessible by trusted devices from anywhere with a high-speed internet connection. Individualized network segmentation ensures the scope of access is limited to that specific customer's devices, eliminating the risk of lateral movement and unauthorized interactions between different AmbuPro customer systems. Network connections are encrypted by AES-256 and completely seamless and transparent to users, regardless of internet gateway, as well as highly resilient to devices disconnecting and reconnecting to the internet.

Dedicated Virtual Server Instances. Each customer deployment within the AmbuPro Cloud utilizes its own dedicated virtual server instance exclusive to that customer and is maintained by OCI Software. This approach ensures that computing resources are isolated, performance is optimal, and potential security risks associated with traditional SaaS shared server environments are eliminated.

Isolated SQL Server Instances. Recognizing the sensitivity of database operations, OCI Software allocates a dedicated SQL Server instance to each customer on the AmbuPro Cloud. Database instance isolation ensures that each customer's AmbuPro database operations are separate and distinct, preventing any unintended records access or interference between different customer databases.

Multi-Factor Licensing, Identity Verification, and Access Control. Multi-Factor Licensing is implemented for an additional layer of security, ensuring that only authorized AmbuPro licenses deployed with a customer code, license key, and single-use secure authorization token are permitted to connect to the customer's environment and AmbuPro database. At any time, with one click, customer administrators can inactivate an AmbuPro license, which prevents AmbuPro application login as well as immediately disconnects and evicts its member device from the customer network. As always, AmbuPro role-based user access to the application is controlled, logged, and audited to ensure records are protected and activity monitored at all times.

Comprehensive Encryption. In addition to network encryption, the AmbuPro Cloud employs AES-256 encryption techniques to protect customer data both in transit and at rest. All database connections from the AmbuPro application as well its mobile synchronization process are encrypted from end to end, including within the customer network. Furthermore, all PHI and PII data at rest is encrypted and unreadable without proper decryption keys. The AmbuPro application and its installers connect via SSL encrypted connections to the AmbuPro License API, which controls and manages network and license access security policies in real time via methods protected by strict JWT authentication/authorization.

High Availability & Disaster Recovery. OCI Software recognizes the importance of its mission-critical AmbuPro customer systems and business continuity in the face of unexpected events. The AmbuPro Cloud implements a robust failover and disaster recovery strategy to ensure the availability of data and services even in challenging circumstances, minimizing the impact of disruptions to its customers.

Least Privilege Access within Customer Instance. Within each dedicated instance, the AmbuPro Cloud strictly adheres to the principle of least privilege access. Users, systems, and the AmbuPro software itself are granted only the minimum level of access necessary for each specific function, reducing the attack surface and enhancing overall security.

Continuous Monitoring & Anomaly Detection. OCI Software prioritizes proactive security measures through continuous scans and monitoring of device, user, system, and database activities. Advanced analytics and real-time anomaly detection mechanisms are in place with the OCI Software Security Operations Center (SOC) around the clock to swiftly

identify and respond to any deviations from normal behavior, enhancing the ability to detect and mitigate potential security threats immediately.

Security Audits & Assessments. To maintain the highest standards of security, OCI Software conducts regular security audits and assessments for all systems within the AmbuPro Cloud. These assessments help identify vulnerabilities, assess the effectiveness of security measures, and ensure the entire ecosystem remains compliant with security standards and regulations.

Secure Software Development Practices. Security is integrated into the entire AmbuPro software development lifecycle. Secure coding practices, regular code reviews, and thorough penetration testing procedures are employed to identify and address security vulnerabilities early and often in the development process.

Summary.

OCI Software's commitment to data security within the AmbuPro Cloud is a central tenet of its operational philosophy. By uniquely delivering dedicated network connectivity and an exclusive virtual server and database instance as well as comprehensive encryption, strict access controls, and continuous monitoring, the AmbuPro Cloud far exceeds healthcare industry standards. As a result, the AmbuPro Cloud provides customers with a secure, trustworthy, and resilient infrastructure for storing, managing, and processing their AmbuPro data.