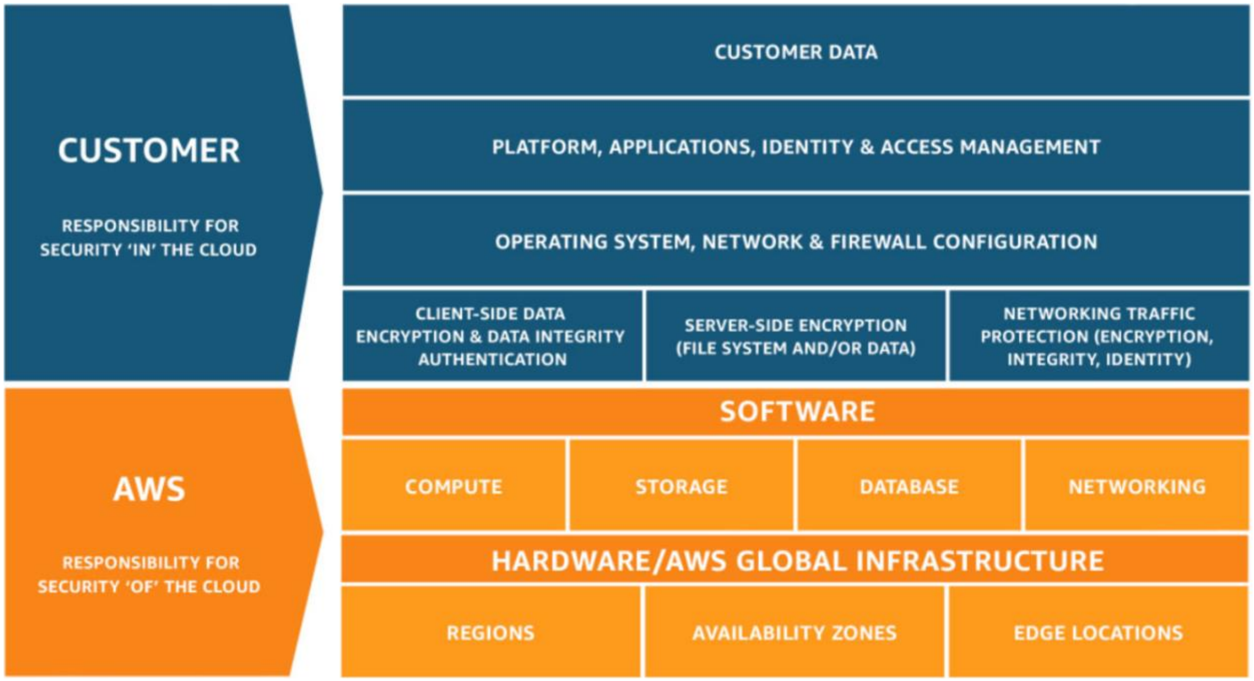
INFORMATION SECURITY & DATA PRIVACY GUIDE

Long-Term Care
DATA COOPERATIVE

1. **What data security and protection does Exponent, Inc., provide?**
   a) Information security and data protection are cornerstones of the LTC Data Cooperative. Exponent demonstrates its commitment to these principles by adopting multiple industry-standard frameworks, such as:
      - A comprehensive security program detailed in the Information Security Management System (ISMS) and Privacy Information Management System (PIMS), which are certified against International Organization for Standardization (ISO) 27001:2013 and ISO 27701:2019.
      - ISO 9001:2015 (and others), which confirms Exponent's commitment to a robust, independently assessed quality management system.
      - National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which serves as an overarching framework for understanding and communicating information cybersecurity.
      - Amazon Web Services, the world-wide industry standard for Infrastructure as a Service (IaaS), by utilizing AWS we are able to ensure best in class physical access as well as leverage the numerous security and privacy standards to ensure compliance with HIPAA, PCI and other standards. This is known as a shared responsibility model.


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Source: https://aws.amazon.com/compliance/shared-responsibility-model/

2. **Does Exponent undergo periodic third-party audits related to its information systems control environment?**
   a) Yes. Exponent undergoes periodic third-party audits at regular intervals, in accordance with industry best practices. These audits include ISO audits, NIST CSF risk and gap analyses, as well as penetration testing. The findings derived from these audit engagements are used to improve the Exponent environment in an effort to maintain the confidentiality, integrity and availability of Exponent's systems and data. Exponent also monitors and audits its security and privacy and information governance people, processes, and controls to ensure compliance with policies and applicable security/privacy standards.

3. **Does Exponent maintain a third-party certification related to its information systems control environment?**
   a) Yes. Exponent maintains an ISO 27001:2013 and ISO 27701:2019 certification that is applicable to its information systems. These certificates are audited and issued by the British Standards Institute (BSI). Additionally, through the use of AWS infrastructure and services, Exponent recognizes the third-party certifications maintained by Amazon Web Services, listed here https://aws.amazon.com/compliance/.

4. **What technical controls are in place to manage use of portable/removable media?**
   a) Exponent's policy requires encryption of all portable/removable media, such as USB storage. All employees are also required to affirm their understanding of the proper use of portable/removable media by successfully completing a graded training exercise. To further protect our systems, Exponent also uses next-generation anti-virus/anti-malware products to analyze all files on any portable/removable media device. Portable/removable media are generally discouraged and Exponent's standard process for data sharing is to use network-based storage mechanisms (SFTP); portable/removable media are not commonly or widely used to transfer data to or from clients.

5. **What processes does Exponent have in place to ensure that administrative controls pertaining to access termination are followed?**
   a) Exponent regularly audits accounts for activity to determine any inappropriate account status. In addition, upon notice of an employee's termination, Exponent's information technology and human resources teams collaborate to configure access expiration, so it aligns with the end of the employee's last day. The staff separation process is initiated through the Exponent human resources system and information technology components are tracked through the information technology ticketing system.

6. **Where do users encounter authentication and what are the password requirements?**
   a) Users must authenticate to any system or cloud service within Exponent's network with authorization granted only to relevant storage or computing environments approved for the user. Data transfers require a minimum of IP address restriction and RSA key cryptography. MFA or other additional layers of security may also be required. Access to and sharing of aggregate, de-identified data requires a minimum of IP address restriction and username/password account authentication.

Exponent will continue to uphold its commitment to quality, security, and privacy by adopting new and emerging risk management techniques as they are available. Should you require any additional detail, please email ltcdc@exponent.com.