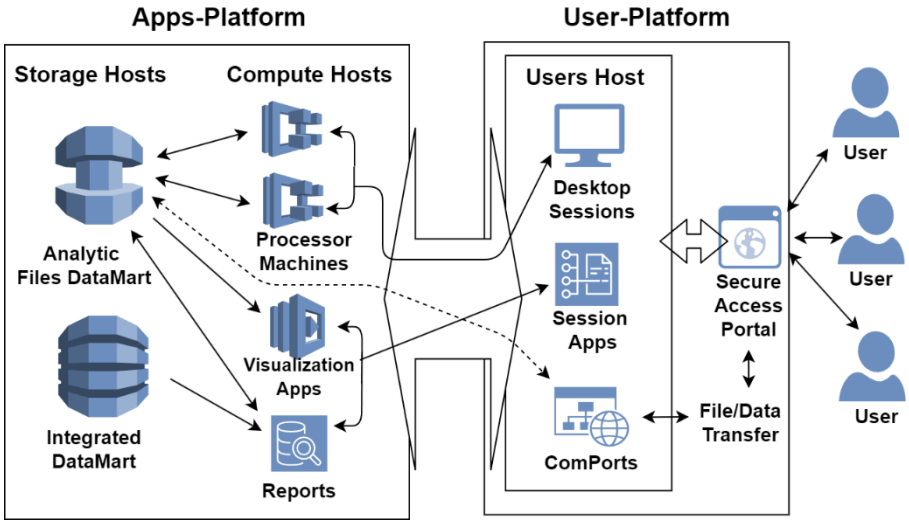
INFORMATION SECURITY & DATA PRIVACY GUIDE

1. **What data security and protection does Acumen, LLC provide?**

Information security and data protection are cornerstones of the LTC Data Cooperative. Acumen, LLC, through its SkyShaper Technologies (SST) information system, demonstrates its commitment to these principles by complying with the moderate-level Federal Information Security Modernization Act of 2014 (FISMA) requirements. The five FISMA compliance requirements include identifying security risks, protecting against a wide range of potential threats, detecting security breaches, responding to cyber threats, and recovering from security incidents. As such, Acumen, LLC maintains the following:

- Periodic Risk Assessments to identify and assess risks to our information systems including threats, vulnerabilities, and potential impacts.
- Implementation of security controls to protect information systems and data including access controls, encryption, and incident response.
- Continuous Monitoring of our information systems to detect and respond to security incidents, assess the effectiveness of our security controls, and maintain awareness of cybersecurity risks.
- A comprehensive security program detailed in the System Security Plan (SSP).
- Compliance with the National Institute of Standards and Technology (NIST) 800-53 rev5 (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final), which serves as an overarching risk management framework for development and maintenance of security and privacy plans for information systems and organizations.

SkyShaper Technologies (SST) User-Platform and Apps-Platform



2. **Does Acumen undergo periodic third-party audits related to its information systems control environment?**

To maintain federal Authorities to Operate, Acumen undergoes annual third-party audits that review their system's security through a Security Assessment and Authorization that verifies compliance with security controls and authorizes the operation of information systems based on risk. In addition, Acumen maintains a Plan of Action and Milestones

(POA&M) that includes security measures and improvements that outlines continuous monitoring and updates to the system. Acumen meets quarterly with the authorizing entities to review this plan and ensure all measures are maintained and/or improved based on the NIST 500-83 rev5 requirements and framework.

3. **What technical controls are in place to manage use of portable/removable media?**
Acumen's policy requires encryption of all portable/removable media. All employees are also required to affirm their understanding of the proper use of portable/removable media by successfully completing annual data security training exercises. Portable/removable media are generally discouraged and Acumen standard process for data sharing is to use network-based storage mechanisms (SFTP) and Application Programming Interfaces (APIs); portable/removable media are not commonly or widely used to transfer data to or from clients.

4. **What processes does Acumen have in place to ensure that administrative controls pertaining to access termination are followed?**
Acumen's enclave system uses access control tools that are used by Acumen and the LTCDC to grant access to Users based on their approval for data access though Data use Agreements issued by the LTCDC Governance Committee. Per FISMA-moderate compliance requirements, Acumen in collaboration with the LTCDC must review and approve users every 90 days to ensure that continued access to data is appropriate.

5. **Where do users encounter authentication and what are the password requirements?**
Users after approval from the LTCDC Governance Committee, are established in a Project Environment. Each Project Environment is entirely segmented from all other Project Environments. The Enclave uses technical protocols designed to prevent a Project and its Users assigned to a Project Environment from accessing or transferring any data, software, or any other form of files from their Project Environment to another Project Environment (i.e., cross streaming of data across Project Environments is not permitted via technical restrictions in place).Users acquire access to the LTCDC Enclave through a User Platform providing secured multi-factor authentication and login. To gain access to the enclave, each user must
    - Establish a secure password (minimum length of 12 characters containing characters from 3 (or more) of the 4 required categories (Uppercase letters, Lowercase letters, Numbers, or Symbols);
    - Review and Accept Acumen's Security Agreement;
    - Undergo Remote Identity Proofing through ID.me or an Online Notary Process
    - Completion of security Questions
    - Establish a multifactor authenticator (DUO Security) to gain access to their enclave account.

    Following the initial account configuration, each user is required to enter their userid, password, and DUO Security code to gain access to the enclave environment. Users will be prompted to change their password every 90 days.

Acumen continuously upholds 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-Support@acumenllc.com.