Policy Name: Member Information	**Policy Number:** 9.1
Section: Information Systems – 9	**Date Revised:** January 1, 2018

9 Information systems

The objective of Alliance Systems Management Unit and Information Systems Unit (SMU/ISU) policies is to ensure the confidentiality, integrity, and availability of Alliance systems and data. ISU staff is located in Durham, NC (Duke University); Rochester, MN (Mayo Clinic); St. Louis, MO (Washington University); and Chicago, IL (University of Chicago). SMU staff is located in Rochester, MN, and Durham, NC. ISU and SMU personnel work collaboratively, maintaining controls at all levels to ensure that all necessary standards are met.

This policy and procedures document contains two parts. *Member Information* describes policies and procedures for Alliance members who require access to the ISU applications, databases and equipment. *SMU/ISU Operations* shows policies and procedures used by the SMU/ISU staff to establish and maintain the applications, databases, and equipment for which they are responsible.

9.1 Member information

SMU/ISU develops and maintains the Alliance Information Systems (IS) that institutional and internal Alliance members use to enter and manage patient and study data. SMU/ISU also manages the Alliance website (http://www.allianceforclinicaltrialsinoncology.org), including the member site, and all Alliance databases. The website provides access to Alliance Web applications and other information useful to members, and is updated regularly as additional Alliance applications and reports are made available. The databases are the repository for member, patient, and study data.

In general, users of Alliance information systems are registered members – persons who assist with Alliance studies or other Alliance mission-related tasks. A primary objective of SMU/ISU is to provide efficient and reliable systems that enable the members to perform their assigned tasks, while safeguarding Sensitive Electronic Information (SEI) and Protected Health Information (PHI), and meeting the requirements defined by regulatory bodies including Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH).

9.1.1 Member account request and setup

All Alliance members must have a Cancer Therapy Evaluation Program (CTEP) ID and a CTEP Identity and Access Management (IAM) account in order to log into the member portion of the Alliance website. Refer to the CTEP website (http://ctep.cancer.gov) or to the Cancer Trial Support Unit (CTSU) website (http://www.ctsu.org) for additional information.

Alliance member accounts give access to the Alliance member site (a restricted area of the Alliance website), and to Alliance IS Web applications. Prior to using the applications, Alliance members must be working with an institution that has IRB approval for an Alliance-based clinical trial, be authorized (as appropriate) to work with a given study's clinical trial data, and receive required Web application training. Alliance Web applications are available to registered Alliance members only. However, users from other research groups may be given access to the Alliance website.

Additional member account setup is also required for user access to the individual legacy ACOSOG, CALGB, and NCCTG websites. Access to the ACOSOG, CALGB, and NCCTG websites is available using links on the Alliance website until the full transition of those functions and content is migrated wholly to the Alliance website. Access to non Web-based applications for staff members is provided by the ACOSOG, CALGB, and NCCTG organizations.

9.1.1.1 Individual institution members

To register a new member and request access to Alliance Web applications, an authorized institution representative must follow the application procedure specified on the Alliance website. During the application process, the prospective member's role assignment(s) is specified. When the application is approved, appropriate accounts are created in the Alliance Information Systems. The member's CTEP username and password is used to access the Alliance member site and SMU/ISU Web applications.

9.1.2 Institution registration

Alliance Institutional membership gives an institution the ability to participate in Alliance clinical trials. Institutional membership requirements and application instructions are available on the Alliance website under the 'Membership' heading.

9.1.3 Alliance application accounts

The Alliance uses Web-based and non Web-based applications for the capture, management, and reporting of clinical data for most Alliance-sponsored studies. As needed, users (who meet the above requirements) from other research groups may be given access to the Alliance website. For all Alliance applications access, an application must be completed and submitted to the administrator who issues access credentials.

9.1.4 User names and passwords

The Alliance requires each user to have a unique user name and password prior to accessing Alliance information systems that contain identifiable patient information. Sharing of accounts or passwords is prohibited. If the Alliance becomes aware of violations, it may be required to report the non-compliance to the offending institution's security officers.

In addition to employing unique user names and passwords, each user must adhere to access restrictions for their accounts, guard their passwords, and change passwords regularly.

9.1.5 Roles and permissions

During Alliance registration, members are assigned roles and permissions that determine the specific Alliance data they may access, and which tasks they may perform.

A member may hold one role or many roles. Roles are defined as group roles, institution roles, committee roles, or study roles. A member holding a role is granted all of the data access privileges defined for the role. When a member holds more than one role, any necessary operation must be defined for access with at least one of the roles held by the member.

Typically, institutional members may access data from their own institutions only. Members from main member institutions can access data from their own institutions and their affiliate institutions. Alliance staff members may access only data necessary to fulfill their job responsibilities.

Members are further granted permissions, which are actions (e.g., read, update) that may be performed on the data they access.

Beyond assigned privileges and permissions, any privilege may be granted, with proper approval, to a specific member. Institutional members who need access to additional data should contact the Alliance Help Desk and request the additional privilege. Help Desk staff will forward the information to Alliance management for approval. Refer to the Alliance website under the 'Contact' heading for Help Desk contact information.

9.1.6 System availability

All Alliance systems are available 24 hours a day, seven days a week, with exceptions for system maintenance. Whenever possible, system maintenance will occur on a planned basis, with one week notice provided to Alliance

members. Unscheduled maintenance may occur as needed to resolve critical security vulnerabilities or to resolve other critical systems issues.

In the event of an unscheduled outage, an SMU/ISU employee will send a message to the established contact lists of users of Alliance systems. If network or internet connectivity problems occur such that users cannot access Alliance systems or send email, an SMU/ISU employee posts a message on the Alliance website under the 'News' heading.

9.1.7 User support

Alliance members require information systems that support all activities related to the conduct of clinical trials. To help meet these requirements, the Alliance provides technical support by trained Alliance Service Center employees to assist users with system, database, Web application, Internet, or study-related problems. Alliance Service Center employees may also create trouble tickets to document user issues prior to assignment to appropriate technical staff.

9.1.7.1 Alliance Service Center

For systems support, the Alliance Service Center is available Monday through Friday from 9 AM to 5:30 PM Eastern Time (8 AM to 4:30 PM Central Time). Refer to the Alliance website under the 'Contact' heading for the Alliance Service Center contact information.

For non-business hour emergency support, refer to phone numbers published in study protocols or memoranda, the Alliance website, and in the Alliance Service Center recorded off-hours message.

9.2 SMU/ISU operations

The remainder of this section contains policies the Alliance SMU/ISU uses to ensure the efficient and effective operation of its computing environment. The policies are divided into the following topics:

- Software development
- Documentation
- Technology selection and change management
- Usage of computing resources
- Security
- Backups and data retention
- Disaster recovery

Alliance IS staff locations adhere to the site-specific institutional IS policies of Mayo Clinic. In many cases SMU/ISU policies and procedures are more restrictive than institutional policies because of the national scope of the Alliance. However, all SMU/ISU policies and procedures serve the best interests of patients and members by providing the highest level of safety and security regarding data collection, maintenance, and reporting. Beyond safety and security criteria, the policies reflect the most efficient and effective means for meeting the goals of the Alliance and industry best practices.

9.2.1 Software development

SMU/ISU develops software applications and interfaces that generate, collect, maintain, and transmit data for clinical trials conducted by the Alliance. The applications are developed using a variety of development tools, technologies, and databases.

ISU uses a tiered software development environment to ensure proper testing and migration from the development to production environments. Software is first deployed to a development environment for initial testing by the software development staff. Software is subsequently deployed to an integration environment for software quality assurance and user acceptance testing, prior to being released into the production environment. New software is deployed during scheduled downtimes unless they are deemed urgent or critical, in which case the software release is migrated as soon as possible.

Completed deployment plans are required prior to implementing upgrades or other software changes in the production environment. Each release is planned to allow thorough testing prior to its deployment to the production environment.

Software developers are required to use development tools that have been carefully reviewed and established as standard within the ISU. Developers use online software development tools to capture project notes, requirements, technical specifications, screenshots, and links to appropriate source code repositories. Developers check all new and modified code into a source code control system that supports team development on various projects, prevents accidental file loss, allows backtracking to previous versions, and manages releases.

Security and confidentiality of study data are maintained at all times. To protect sensitive and confidential information, applications incorporate sound security practices and comply with HIPAA guidelines. All Alliance applications safeguard protected health information (PHI) by requiring secure logins, limiting access to authorized users, and implementing encryption schemes for data transmission.

9.2.2 Documentation policies

Documentation may include but is not limited to user manuals, job aids, training manuals, development documentation, policies, and standard operating procedures. All SMU/ISU documentation – whether in-process or released – is housed in a common server location.

During documentation development, writers follow consistent documentation templates. Documents intended for external (non-SMU/ISU) audiences are reviewed by the Training Team before they are finalized for publication. The reviewer list is dependent upon the document content.

9.2.3 Technology selection and change management

As resources permit, the Alliance works to maintain a state-of-the-art computing environment. Alliance developers use open-source software customized to Alliance needs, or software developed in-house. In some cases, commercial software solutions are a better choice, and are used if the vendor places a high priority on integration capabilities. The Alliance does not use commercial systems provided by a single vendor that would create a closed environment.

SMU/ISU projects are prioritized by the SDC Directors and monitored through Program Operations.

9.2.4 Usage of computing resources

9.2.4.1 Alliance staff and members

As part of its mission, the SMU/ISU acquires, develops, and maintains computers, databases, and networks. These computing resources are intended for Alliance-related purposes, including direct and indirect support of the Alliance mission.

Use of Alliance computing resources is not completely private. While the Alliance does not routinely monitor individual usage, normal operation and maintenance requires the backup of data and communications, the logging of activity, the monitoring of general usage patterns, and other activities necessary for the provision of service. Under prescribed circumstances, the Alliance may also specifically monitor the activity and accounts of individual Alliance computing resource users, including individual login sessions and the content of individual communications.

The Alliance does not permit use of its computing resources for personal, financial, or other gain.

9.2.4.2 Alliance staff

Alliance staff housed at institution locations must adhere to locally established usage requirements.

9.2.5 Security

SMU/ISU uses industry best practices to protect information against unauthorized access, use, or destruction. Access is controlled in order to limit the exposure of sensitive patient data.

Four categories of access control are implemented:

- Facilities
- Network and servers
- Database
- Application (includes Alliance website(s) and Web applications)

For all users, the SMU/ISU completes an Alliance authorization and account creation process before physical or electronic access is granted.

When a user no longer requires access, and authorization to terminate an account is received, SMU/ISU Help Desk employees terminate the user's role(s) and disable accounts that provide access to the Alliance software applications.

9.2.5.1 Alliance Statistical Center facilities security

Permission to access to the Alliance Statistical Center facilities is determined by local institution guidelines.

The Alliance Data Center is a high security environmentally controlled and monitored computer room within the Statistical Center. Access to Alliance Data Center facilities is controlled through use of an Access Identification Card provided to permanent staff or vendors who have management authorization to be at the Data Center and have received training. Vendors may be approved for temporary or long-term access. Visitors that require access to the Data Center must receive management pre-approval and must sign in at the wall-mounted computer near the entrance to the facilities. In addition, visitors must be escorted during their visit by a cardholder with Data Center access authorization.

The Alliance monitors for and protects its computer resources against environmental hazards. Systems are centrally monitored, kept in temperature-controlled conditions, and are protected against electrical power surges and short-term outages. Backup generators are available onsite to ensure the continuous operation of the Data Center in case of long-term utility power failures. To comply with local building and fire codes, computer resources are protected by automatic smoke detection and fire suppression equipment.

9.2.5.2 Network and server security

SMU/ISU passwords and network/server security upgrades must be managed to conform to local institution practice.

Alliance systems housed at the Statistical Center are protected by enterprise firewalls and network security, which provides continuous monitoring to identify and prevent malicious access.

Server login passwords are encrypted and stored in their encrypted form in protected files.

An administrative user account is a specific account type that allows access for system administration purposes, including setup of user accounts. Administrative users only are authorized to manage accounts and servers. An Alliance computing manager responsible for specific work units designates Alliance SMU/ISU staff administrative users and assigns them a unique user ID and password.

9.2.5.3 Database security

Because of the highly sensitive nature of data collected by the Alliance, and the right to privacy of patients entered on clinical trials, only authorized members with a need to know will be given access to data in the Alliance databases. SMU/ISU ensures the security and integrity of the databases through password controls, logging, monitoring, and auditing.

SMU/ISU implements database auditing for relevant features related to data definition, security administration, and logon failures. The SMU/ISU implements both database and application level auditing for relevant features related to data manipulation, security administration, and logon failures. A database audit trail is used to record date, time, and user for various levels of standard and suspicious activity. A correction history is available to record date, time, and user for all data manipulation activity.

SMU/ISU monitors each database product software lifecycle, and ensures that appropriate updates are applied. Each new release and version of the database software is identified, considered for installation, and installed after rigorous validation.

For database patches, SMU/ISU follows industry best practices. Database security patches are installed only after they are validated against the SMU/ISU computing environment. If validation is successful, installation will occur as soon as possible after the date of release.

Database user accounts are set up after authorization by the appropriate manager. Database passwords expire at preset intervals per institution standards and must be changed when required. SMU/ISU employees inactivate or remove user accounts immediately upon notification of termination of employment or Alliance membership.

9.2.5.4 Application security

SMU/ISU develops and/or supports software applications for use by Alliance members. These applications enable such functions as patient registration, specimen tracking, reporting, and data entry and review. ISU applications encrypt all data transmission to ensure security and confidentiality of data as it is entered and viewed.

Authentication and authorization services ensure consistent security for applications. Users are provided accounts and roles that determine their access, at a granular level, to data and functions. These roles are periodically reviewed by SMU/ISU directors, with final approval for changes given by the Alliance IT Committee.

9.2.6 Backups and data retention

All system and database backup and recovery procedures adhere to industry best practices. Alliance data is safeguarded against loss via industry standard backup and retention schedules. Backups are performed on a daily basis. Using the backup scheduler and policy engine, data backups are targeted to a tape library located in a remote data center physically separated from the primary infrastructure hosting Alliance application and data services. Data are retained for a period not less than 30 days. Alliance employee workstations are managed by local desktop support and fall under the backup policies of the support environment.

9.2.6.1 System and database backups

Controlled and monitored backup rotations protect all servers, file storage devices, and server security information.

9.2.6.2 Servers

Servers are designated by institution policies as critical or non-critical. All servers receive a weekly full backup, and incremental backups. In the event of file loss, file corruption, or total equipment loss, SMU/ISU is able to recover from the previous full and incremental backups. Maximum file loss would be 24 hours.

9.2.6.3 Retention and storage

Backup tapes are retained for two months. Longer data retention is additionally determined by the study. Security access files for all

machines supported by the SMU/ISU are backed up and retained as required by HIPAA.

Backups are stored offsite from the main data center. Statistical archives are stored in SAS data sets rather than in the Alliance database and are housed on a separate server.

9.2.7 Disaster recovery

The Alliance has a formal disaster recovery plan to be used in the event of a significant failure of regular computing services. The plan identifies the primary and backup members of the disaster recovery assessment team and the functional systems area for which each person is responsible. If an event occurs that requires the attention of the team, all members assemble to begin an assessment of the situation for their respective area and prepare an estimate of the time and level of effort required to restore operations. Restoration efforts are directed by the ISU leadership. Recovery time will depend on the nature of the disaster.