### Office of Information Technology

Emory University’s Office of Information Technology (OIT, formerly LITS) is Emory University’s central Information Technology department, supporting all missions of research, healthcare, education, and administration.  OIT consists of professional information technology employees and manages all technical infrastructure (networking, data centers, service centers, etc.), information security infrastructure, enterprise-wide applications, healthcare delivery systems, and enterprise research platforms.

*Research IT Environment*

Emory University operates a high-speed, research information technology infrastructure to support the research mission of the University.  With a high speed ten gigabyte fiber as its backbone, the network provides speeds of up to a gigabyte to the desktop and ten gigabytes throughout the internal campus with several points of redundancy through to the commodity Internet and Internet 2.  Physical servers and hardware are stored in a 24x7 monitored professional data center with environmental and physical controls in place.  The University hosts a virtual server farm and petabytes of storage that can quickly be provisioned based on investigator needs.  From a security perspective, Emory University adopts a defense-in-depth strategy incorporating security and privacy controls at a policy, operating system, network device, and intrusion prevention systems.  The University has HIPAA compliant network zones and infrastructure in place and implements encryption mechanisms to secure sensitive data at rest and in transit.

In recent years, Emory has developed a partnership with Amazon Web Services (AWS) and built AWS at Emory - a customized environment and service to offer cloud computing and storage resources for a variety of research and teaching use cases. AWS at Emory provides investigators with access to many of the key research computing services offered by AWS and provides additional security and technical controls to help ensure the data are protected from unauthorized use. Within this environment, investigators and their team are able to take advantage of the scalability and elasticity of the cloud while leveraging best practices in cloud computing.

Some highlights of the service include:

* When using AWS at Emory from on campus, the traffic flows through the Emory core network to the AWS environment. Throughout the Emory network, the network devices are redundant to ensure a high standard of availability. In addition, wherever appropriate, the network traffic will flow over the Internet2 pathways to take advantage of the high speed, restricted academic network.
* As part of the account creation process, the service provisions a set of virtual private cloud environments that provide geographic redundancy for the data and services. Through this automated process, the environments are set to an approved configuration with minimal risk of variations. With all steps automated, there is a greater level of assurance around firewall rules, network configurations, and environment set ups.
* All AWS services enabled in AWS at Emory have been assessed by the Emory Information Security team for potential risks. Where applicable, the teams have built out monitoring and remediation controls to check to ensure the accounts do not implement configurations that may have unintended consequences or move them to a state of non-compliance. For example, all storage must be encrypted. If the storage is configured to be not encrypted, the monitor will notify the account owner and dismount the storage.

In addition to these Emory-specific customizations, Emory research teams benefit from: (a) Amazon’s elasticity, providing investigators with the opportunity to scale up or scale down their infrastructure based on needs. As such, the team is not paying for unused or idle infrastructure; (b) ability to tap into Amazon’s technology optimized for specific research workloads, such as high memory computing cores and high speed solid state drives (SSD); and (c) quickly spin up computing resources within minutes to increase the time for investigators and their team to conduct their science. In support of this service, Emory has dedicated technical resources to help researchers and their teams. Emory has purchased AWS Enterprise support to provide 24x7 support for the service, and is also sponsoring training and leading a cloud community of practice, which includes participation from investigators, IT organizations, and scientific cores.

*Research Data Systems and Applications*

Data systems and applications used for research purposes can be hosted and administered on Emory OIT servers, either physically or through Virtual Machine environments.  Emory OIT implements best practices in application management and support, such as maintaining application, database and web interface components on separate servers, establishing backup / fail over server redundancy for service continuity and system and data recovery, and maintaining distinct development, test and production environments for efficient application testing, upgrade and deployment.  Access to systems in the Emory network zone is supported by secure VPN connection and remote access tools, and by state-of-the-art technology for identity management and authentication, and account credentials encryption.  Role-based permission controls ensure that users have appropriate access to the designated functions and data records in applications and underlying databases, including row-level partitioning when necessary.  Emory OIT applies regular functionality and security software, hardware and operating system patching and upgrades, according to existing policies and program-specific service-level agreements.

A variety of Enterprise applications and services are supported by Emory OIT to enhance the research experience and allow teams to capture, analyze and disseminate data in a reliable and secure way. Examples include: the REDCap data capture system, the Emory Laboratory Information Management System (LIMS), the OpenSpecimen biobanking application, the Tableau data visualization application, the Salesforce customer relationship management platform, the DocuSign electronic signature application, and more. In partnership with Emory’s Biomedical Informatics department and in support of the Georgia Clinical and Translational Sciences Alliance, Emory OIT operates an instance of the i2b2 platform and an installation of the TriNetX system – both sourced from de-identified and aggregated Emory Healthcare electronic health record data for prospective patient cohort discovery that fit certain eligibility criteria.

Research applications that make use of patient health information are not directly connected to the electronic medical record system.  Instead, applications may draw on data extracted from the Emory clinical data warehouse read-only environment maintained by Emory Healthcare Information Systems, or on data abstracted from data instruments and entered in research applications and databases maintained by Emory OIT, such as the REDCap data capture system, the Emory Laboratory Information Management System and OpenSpecimen biobanking application, and program-specific data repositories.  The release of health record data for a research study necessitates approval from the relevant Institutional Review Board, Research Oversight Committee and Healthcare Medical Records instances.  When required for a particular study, data de-identification and date-shifting processes are applied to datasets in compliance with removing HIPAA identifiers before their transfer to investigators or partner institutions, as specified in data use, sharing and transfer agreements.

Any OIT-hosted application is approved for deployment by an Architecture review committee and a Security review committee, which assess the soundness and detailed integration of the application within the Emory infrastructure, including its ability to meet HIPAA regulations with minimum risk, as documented in a HIPAA risk assessment and risk remediation plan.  In addition to being hosted on Emory HIPAA-compliant servers, data systems and applications are provisioned to a list of pre-authorized users associated to a study IRB protocol, with specific privileges regarding access to functionality and particular data records.  Additional administrative super-user accounts are granted to the application and / or the underlying database to perform application configuration, maintenance, troubleshooting and other user support tasks, as necessary.  Any OIT personnel accessing sensitive data is required to be CITI and HIPAA certified and operates under an Honest Broker protocol.