### Office of Information Technology (Overview)

Emory Office of Information Technology (OIT) 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 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.
* **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 two-factor authentication VPN connection and remote access tools, and by state-of-the-art technology for identity management, 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 whenever deemed necessary. Emory OIT applies regular functionality and security software, hardware and operating system patching and upgrades, according to policies and program-specific service-level agreements.  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 OIT, such as the Redcap data capture system, and program-specific data repositories.