Icahn School of Medicine at Mount Sinai

ICAHN SCHOOL OF MEDICINE AT MOUNT SINAI
DATA CYBERSECURITY SAFEGUARDING MEASURES,
RISK ASSESSMENT AND MITIGATION CONCERNING
STUDENT INFORMATION

Introduction

Icahn School of Medicine (ISMMS) is committed to ensuring a safe cyber-environment for its student information, recognizing that the risks of cyber threats are continual and high. ISMMS regularly monitors risk factors and implements security measures to safeguard student information and to mitigate potential new risk. ISMMS utilizes the Empower Student Information System to provide, process, and retain student bio-demographic, educational and financial information. Empower's parent company, ComSpec, utilizes cloud-technology and is responsible for the software's design and maintenance. ISMMS has identified the Associate Dean for Enrollment Services as the business owner of the school's student information system technology. They, in concert with the Division of Academic Informatics and Libraries, evaluates the student information system and manages its risk assessment safeguard plan.

Plan

Three major potential risk elements have been identified: employee training and management; information operating system information processing, storage, transmission, and disposal; and, the detection, prevention and response to attacks, intrusions and other system failures. To address these risks, the following safeguards have been implemented.

Potential Risk Element: Employee Training and Management

Safeguard Initiatives:

a. All new employees participate in a required orientation program that includes information on data security management.
b. All employees must complete a mandatory set of annual corporate core compliance education plan. These courses include fundamental modules on data security, permitted uses and disclosures of data, preventative measures to take when accessing protected information, the dangers of phishing, and recognizing risks of malware. The Associate Dean for Enrollment Services ensures completion of the annual corporate core compliance education plan is completed for all staff.

c. Access to the student information system is password protected; access controls are utilized to limit access to student specific data and associated transactions to only relevant business units and positions; and, access is rescinded after an employee is terminated.
d. Additional annual advanced training modules are required of staff with access to the student information system on the topics of malware, ransomware, and spear phishing.

Potential Risk Element: Information Operating Systems – Information processing, storage, transmission and disposal

Safeguard Initiatives:

a. The Academic IT Support Center (ASCIT) routinely provides security updates of operating systems, applications, and endpoint security. Updates are scheduled off-hours to ensure a minimum impact on daily operations. Endpoint security, including running antivirus and anti-malware, is part of the automatic scheduled security maintenance activities.
b. Proactive monitoring of the operating systems and networks for vulnerabilities is conducted by the Mount Sinai Health System (MSHS) Information Technology Department on an ongoing basis.
c. The Associate Dean for Enrollment Services serves as co-chair of the ISMMS Academic IT Steering Committee and provides information to ISMMS leadership regarding student information system concerns.
d. All electronic documents concerning student information are stored on shared drives, with servers monitored and managed by the MSHS Information Technology Department.

Potential Risk Element: Detection, prevention and response to attacks, intrusions and other system failures

Safeguard Initiatives:

a. The Associate Dean for Enrollment Services works closely with the Vice President for Information Technology/Senior Associate Dean for Research and Academic Informatics to address concerns relating to detection, prevention, and response to information system failures that may affect the ISMMS student information system. Strategies to enhance the safeguarding of student information from system attacks are reviewed, with action plans developed and implemented to mitigate potential risks from internal and external sources.
b. Annual meetings are held with the leadership of ComSpec to ensure appropriate safeguards are in place with respect to data security from system attacks for ComSpec's areas of responsibility.