System and Communications Protection Policy

- Purpose
The System and Communications Protection Policy, guides the use of cryptography to ensure the confidentiality and integrity of information stored in systems as well as in transmission. It also describes the suggested data flow to support the security of information.

- Scope;
This policy will apply to all of Mount Sinai Health System and its associated entities.

- Roles and responsibilities;
  o Management will:
    o Oversee implementation of this policy.
    o Ensure that exceptions to this policy are documented with Information Technology Security.
    o Provide training, in conjunction with Information Technology Security, to their constituents.
  o Information Technology Security will:
    o Maintain this policy in accordance with NIST guidelines to benefit the Mount Sinai Health System.
    o Review the policy, its articles and procedures annually or as is deemed necessary.
    o Support training activities having to do with this policy.
  o Application Owners will:
    o Establish classifications (PHI/PII) of data stored, processed or moved through systems.
    o Ensure that data handling controls are implemented and followed.
  o Authorized Users will:
    o Only access authorized systems and data.
    o Only assume privileges for which they are authorized.
    o Protect the systems, or information contained on systems, at the level in which it has been classified.
    o Share access to the system, or information contained within, with only authorized personnel.
    o Report any suspected, or actual, un-authorized access to their management team.

- Policy
Publicly accessible information systems at The Mount Sinai Health System are relegated to the demilitarized zone of the infrastructure. This adds an additional layer of security between the Internet and intranet systems.
The Mount Sinai Health System prevents the unauthorized removal of information across managed interfaces by use of a data loss prevention mechanism.

The Mount Sinai Health system protects the confidentiality and integrity of information at rest by making full disk hard drive encryption a part of the managed build process when practical. In addition to this, all portable laptops should have full disk encryption enabled to prevent data loss or unauthorized disclosure of information at rest.

At least annually the System and Communications Protection Policy will be reviewed and updated by management to ensure its continued effectiveness. Otherwise, in the event that significant regulatory change occurs, the policy will be reviewed and updated as needed to ensure compliance.