Statement of Policy

Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objectives

The goal of these policies and guidelines is protect our patients' health information and other protected information such as individually identifying information or financial information ("Protected Information") by enhancing the security of our electronic information systems. WashU requires securing Protected Information contained on all mobile media, laptops, workstations, servers and external hosted sites that are not located in Approved Secure Data Centers. Approved Secure Data Centers are defined as data centers that have had a formal risk assessment on the physical and logical controls completed by the Information Security Office and the Internal Audit Office with no findings that would render the data center unsecured.

Applicability

These policies and guidelines apply to all workforce members who use, collect and/or access Protected Information. These policies and guidelines apply to all University owned and personal electronic devices that are connected to the WashU networks and receive, store or transmit Protected Information. This policy does not cover text pagers or basic voice / SMS text cell phones.

Policy

All electronic devices that receive, store and/or transmit Protected Information and are not located in an Approved Secure Data Centers must use WashU-approved encryption methods to secure the information stored on or transmitted outside the secure clinical network.

- Servers that are not located in an Approved Secure Data Center are required to have all information stores of protected information encrypted.
- Protected Information contained on laptops or workstations are required to be either File,Folder or Full Disk Encryption.
- Any and all mobile devices e.g. smart phones and tablets that connect to the secure clinical network that may contain or transmit Protected Information (e.g. e-mail) are required to accept Information Security Standards to encrypt and protect the devices. External storage media (i.e. backup tapes, removable drives, etc) will need to have the Protected Information encrypted.
- Files that contain protected information that are transmitted across the Internet (e.g. e-mail attachments sent to non-WashU or BJC addresses, or file transfers to other entities) will need to have the attachments encrypted or use a WashU secure encrypted method to deliver that information.

Exceptions

Existing systems and applications containing Protected Information which cannot use encryption because of technology limitation but have compensating controls may be granted a special exception by the Information Security Office (ISO). However, these systems and applications will be required to have a formal risk assessment performed by the ISO to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.

Title: Encryption Policy
Version Number: 1.2
Creation Date: June 3, 2011
Applicability: Protected
Reference Number: 02.05
Status: Final Revision
Date: May 11, 1016
Policy Owner: Information Security Office