Policy

All members of the Weill Cornell Medical College (WCMC) community are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by the college. WCMC reserves the right to restrict the use of Information Technology Resources in order to preserve data security or comply with law or policy.

In order to further secure data and improve regulatory compliance, WCMC has implemented Data Loss Prevention (DLP). WCMC uses DLP to identify confidential data on the WCMC network and – in cases where intentional or unintentional use violates policy – block the creation, reception, storage or transmission of confidential data.

Reason for Policy

DLP is an automatic surveillance system that consistently watches activity on the network and on WCMC desktop and laptop computers. It identifies confidential data (e.g. patient health information, social security numbers, and credit card numbers) and flags it for further investigation. In some cases DLP will stop the flow of data (e.g. if an email containing confidential data is sent to an inappropriate recipient, DLP may be used to temporarily or permanently block that email).

DLP has the ability to:

- Monitor **data in motion** (e.g., emails and instant messages)
- Search for and analyze **data at rest** (e.g., data residing on a file server or database) and **data at the endpoint** (e.g., files on a laptop, desktop, or in a flash drive).

By gathering this information, DLP can determine if data is confidential (refer to the ITS Data Classification policy), and appropriately secure it to prevent security policy violations and maintain regulatory compliance.

WCMC handles a large amount of confidential data on a daily basis. Technologies that enable WCMC to function efficiently and make data easy to access and share also increase the risk of unauthorized disclosure and loss of confidential data. This has potentially serious consequences, including financial penalties, customer dissatisfaction, increased regulatory scrutiny, and reputational damage.

DLP is being used in conjunction with other security tools to protect confidential data and reduce the risk of it being compromised. This helps protect both the data that our organization is in charge of as well as the WCMC community from the consequences of losing confidential data.

Entities Affected By This Policy

The Weill Cornell Medical College and Graduate School of Medical Sciences

- Responsible Executives: WCMC Chief Information Officer
- Responsible Department: Information Technologies and Services
- Dates: Interim Issued: *April 7th, 2011* Final Issuance: *April 7th, 2011*
- Contact: Information Technologies and Services

Principles

Certain information such as patient health information, personnel data, or financial records is confidential and must be treated with extreme care to avoid inappropriate disclosure with possible attendant fines or mandated notifications.

WCMC community members should not expect that personal communications will remain private and/or confidential. While the college permits generally unhindered use of its information technology resources, those who use WCMC information technology resources do not acquire, and should not expect, a right of privacy.

A complete list of all data considered confidential by WCMC is available here: http://weill.cornell.edu/its/policy/security/11-3-data-classification.html

Procedures

DLP is already actively monitoring both data in transit and at rest on the WCMC network, including (but not limited to):

- Email
- Webmail
- HTTP (message boards, blogs and other websites)
- Instant Messaging
- Peer-to-peer sites and sessions
- FTP

WCMC community members should continue to abide by existing policies for appropriate use of ITS resources as provided in the ITS policies page: http://weill.cornell.edu/its/policy/.