Merge Healthcare
Information Security Summary

A statement regarding the controls in place to protect the confidentiality, integrity and availability of information owned by and entrusted to Merge Healthcare.

Contact Information:

Security Officer

Scott Sippel

(262) 369 3387

Scott.Sippel@Merge.com

IT Security Manager

Bruce Coulter

(262) 912 3418

Bruce.Coulter@Merge.com

MERGE

Version 1.0
Updated on 7/10/2013
Prepared by Bruce Coulter

Overview

Merge Healthcare Incorporated (referred to herein together with its affiliated companies as "Merge Healthcare" or the "company") has in its possession a wealth of information—including information about its customers, employees (both past and present) and many others. The protection of this information is of critical importance to maintain its confidentiality, integrity, and availability. Merge Healthcare has applied numerous security controls which help to ensure that all information within the company's custody is properly and adequately protected.

Merge Healthcare demonstrates its commitment to information security by:

- Dedicating security resources in terms of staff, budget, and technology.
- Investing in highly available and recoverable systems and facilities.
- Investing in security technology.
- Continually seeking to evaluate and improve procedures related to security.
- Adopting policies, communication and training related to end user awareness.
- Striving to maintain compliance with all applicable legal and industry requirements.

Security Policies and Standards

Merge Healthcare utilizes published security policies and standards to support business objectives within its information systems and processes. These policies and standards are implemented, communicated, and reviewed on a regular basis and are a reflection of the executive management team's commitment to information security. Policies and standards are in place to govern the protection of the company's information assets and any information assets of our customers (and others) that have been entrusted to Merge Healthcare.

Human Resources

Merge Healthcare employs a dedicated information security staff whose sole responsibility is the protection of information. In addition, it is the responsibility of all employees to be aware of information security issues within their daily work. In order to promote awareness, Merge Healthcare employees are required to complete training on the company's security policies, their responsibilities to protect the confidentiality of information entrusted to them, appropriate use of resources, extra care required for the protection of mobile devices, and other related topics. All employees are subject to background checks as a condition of employment.

Confidentiality Agreements

Merge Healthcare enters into confidentiality or non-disclosure agreements with its vendors, contractors, employees and clients to contractually safeguard personal and other confidential information belonging to Merge Healthcare or in Merge Healthcare's custody.

External Reviews

On a recurring basis, Merge Healthcare is audited by independent third parties in order to maintain compliance with laws and regulations such as the Sarbanes-Oxley Act, HIPAA and the HITECH Act. Annual risk assessments are performed to help the company identify any potential risks to its information assets and to help prioritize efforts to mitigate those risks. The overall information security program is also reviewed and evaluated against the ISO/IEC 27000 Family of Standards.

Periodically, the company also engages external firms to perform more in-depth evaluations of its security controls by conducting penetration testing and other similar exercises.

Internal Reviews

In addition to external reviews, internal tests are conducted on a regular basis to ensure compliance and verify control effectiveness. Monthly vulnerability scans are conducted, and the results of these scans are used to identify vulnerabilities to be addressed.

Physical Security

All data centers hosting Merge Healthcare information (or information that is managed by Merge Healthcare on the behalf of others) are secured structures protected by defined security perimeters. These facilities are protected by physical security barriers and entry controls designed to prevent unauthorized access, damage, and interference. Fire suppression, environmental controls, and redundant power supplies are all in place, as are CCTV cameras to monitor the facilities and all entrances to them.

Operational Security

Responsibilities and procedures for the management and operation of information processing facilities are established and separation of duties by function across the organization has been implemented.

Operational change to systems is controlled through various defined change management processes.

Access Control

Access to information, information processing facilities, and business processes are controlled on the basis of business and security requirements. Access control rules take into account the basic principle of “need-to-know” and the sensitivity of corporate and personal information.

Layers of security controls limit access to information. These include controls at the network, application, operating system, and database levels. Passwords are used in conjunction with each of these layers; they are subject to defined password construction rules and must be changed at regular intervals. Password administration and management are controlled processes that generate automated audit records.

Data Communications Security

Technologies such as PGP, SSL (TLS), and IPsec are used to encrypt data when in transit over public networks. The use of such technologies is dependent upon the level of sensitivity of the information, both corporate and personal.

Computer Security Measures

Various security technologies are deployed within the infrastructures and include firewalls, anti-virus, anti-spyware, and intrusion detection systems and processes.

Security data is logged and regularly reviewed to identify policy violations and security incidents. Incidents are documented and investigated to determine severity, root cause, and follow-up actions required. Measures to be taken to prevent re-occurrence are also identified, documented, and implemented as needed.

Disaster Prevention and Recovery

Adequate back-up capabilities exist to ensure that all essential information and software can be recovered following a disaster or media failure. Backup information is stored at a remote secure location, at a sufficient distance to escape any damage from a disaster at the primary site. Backup media is protected against unauthorized access, misuse or corruption during transportation beyond the data center boundaries.

Combinations of preventive and recovery controls are implemented to help protect from harm due to loss of data or processing capabilities. These controls are designed based on an assessment of risk, and are meant to keep the harmful effects of any outages to a minimum. The processes making up these control measures are tested on a regular basis.