Information sensitivity and protection of data

Technology, Information Technology

Information Sensitivity and Protection of Data Introduction Information that causes penalty, losses, personal invasion, or indiscreetness once handled inappropriately requires assignment of high sensitivity level of access and protection concerning who has access to it. Major organizations apply almost similar protection and handling policies and in this case, we are going to be analyzing the strategies set by three leading healthcare organizations: Beth Israel Deaconess Medical Centre, Mayo foundation and Georgetown University by comparing their rules and regulations in data handling.

The outline of policies that Mayo Foundation uses in handling sensitive data, as appears in Managing Information Privacy & Security: Mayo Foundation (2002) is:

There is a dedicated group running a program to oversee security policies and standards of Mayo’s general information.

There are strict standards of ethical use of information, information resources, and authorization over specific information.

Mayo has strong access controls to physical and electronic information and their resources. These measures protect vital information from unauthorized access, disclosure, or circulation.

Mayo protects and controls any information that it transmits outside, mostly electronic, and puts measures to ensure ethical, harmless, and authorized transfer or sharing of its information.

There is emphasis on integrity with regard to vital information that prevents it from errors, unauthorized reproduction, alterations, and destruction.

Mayo has measures that prevent information loss like back up systems and lost information recovery abilities.

The policies that Georgetown University Medical Centers uses in handling sensitive data, as appears in Managing Information Privacy & Security: Georgetown University Medical Centers (2007) are:

There university protects the privacy of all the health information it creates, acquires, or maintains.

It protects the rights of patients in accordance to disclosure and use of their medical information.

It restricts its personnel from using or disclosing protected health information in inconsistent manners.

Amending of patients' medical information is allowed, but after requests and considerations are made.

It restricts use or disclosure of information to components of the university that are not health care components.

Access of information is only to personnel dealing directly with the case.

There are policies to limit extensive use of protected information beyond the university.

The policies that Beth Israel Deaconess Medical Center uses in handling sensitive data, as appearing in Managing Information Privacy & Security: Beth Israel Deaconess Medical Technology Resources Policy (2007) are against the following:

Unauthorized access, monitoring, decoding, and filtering of its data network.

Entering designated data rooms without permission.

Interfering with physical or logical components of the data network.

Exposing the data network to vulnerabilities such as virus.

Alteration of electronic information or data.

Disclosure of vital information via electronic means such as email.

Common themes observed in the three organizations

Access to vital information is a key concern by these organizations. There are policies put in place that emphasize of access of information to authorized personnel only. In most cases, there are access control measures allowing specific personnel access to them. Hacking or breaking into somewhere are means of accessing information illegally, leading to further means of access control such as power switches and anti-hacking software. Disclosure of crucial information is critical in healthcare. It may have serious consequences on the patient or their relatives (Herdman, 2006). It is therefore wise to keep it as discreet as possible. In large firms with different departments, restricting disclosure to the less involved ones is a possible way of curbing disclosure. There are also restrictions of unauthorized disclosure of institutional information beyond it, mostly by export through electronic means.

The issue of data alteration is a key concerning the three organizations. Altering data interferes with crucial conclusions or actions of healthcare institutions (Iyer, Levin, Shea & Ashton, 2006). Alteration occurs intentionally by malicious staff and is preventable by having monitoring systems such as CCTV cameras in safe rooms. Accidental alterations occur in some cases such as virus attacks on databases, leading to restriction of digital uses that may expose information to such. Destruction of data is likely to occur in any organization in form of crises such as fire, system failure, or virus attacks. Luckily, these are preventable by having fire-fighting equipment, computer back up systems and proper anti-virus software, or in the case of electronic

data loss, data recovery mechanisms are available.

It is evident that most of the policies applied in data protection are very similar. The observable differences are only observable in the preference of prevention tactics. For instance, one organization goes for CCTV monitoring systems to curb the issue of unauthorized entry of staff into restricted areas whereas the other uses automatic card registration doors to lock them.

The policies that enforce control and protection of information so that only those who need it for professional use access it are very important. It is evident from the essay that most of the violations to sensitive information occur within an organization. Therefore curbing this problem will go reduce the violations by a significant margin. In addition to the internal solution, incorporating a system of detecting and warning in case of attacks to an information system is a major element in solving this issue. This is quite important owing to the fact that the world of technology fluctuates fast and being outdated on preventive measures leaves information prone to exposure, damage, and loss.

References

Herdman, R., Moses, H. L., National Cancer Policy Forum (U. S.), & United States. (2006). Effect of the HIPAA privacy rule on health research: Proceedings of a workshop presented to the National Cancer Policy Forum. Washington D. C: National Academies Press.

Iyer, P. W., Levin, B. J., Shea, M. A., & Ashton, K. (2006). Medical legal aspects of medical records. Tucson, AZ: Lawyers & Judges Pub. Co.

Managing Information Privacy & Security: Beth Israel Deaconess Medical Technology Resources Policy (2007). HIMSS. Retrieved on October 17, 2013

from http://www. himss.
org/content/files/CPRIToolkit/version6/v6%20pdf/D39a_Beth_Israel_Deaconess_Medical_Center_Technology_Resources_Policies. pdf

Managing Information Privacy & Security: Georgetown University Medical Centers (2007). HIMSS. Retrieved on October 17, 2013 from http://www. himss. org/ASP/privacySecurityTree. asp? faid= 78&tid= 4 and http://www. georgetown. edu/policy/hipaa/privacy. html

Managing Information Privacy & Security: Mayo Foundation (2002). HIMSS. Retrieved on October 17, 2013 from http://www. himss. org/content/files/CPRIToolkit/version6/v6%20pdf/D39e_Mayo_Foundation_Information_Security_Policies. pdf