ENSURING COMPLIANCE TO HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) USING E-SAFE COMPLIANCE

Author: Ahmad Jawwad

Published: June 2017

INTRODUCTION

As health information security policies are emerging under different standards, such as Health Insurance Portability and Accountability Act (HIPAA), ISO/IEC 27002 etc., healthcare organisations are required to ensure the security of electronic health information, or electronic medical records (EMRs), and to control their access. Any healthcare provider must apply security measures and safeguards that allow it to implement the necessary standards for protection.

The solutions used, or safeguards applied, for protecting health information can be:

i) administrative (e.g., training of workforce)[1],
ii) physical (e.g. installation of controls to facility)[2], or
iii) technical (e.g. implementation of new technology)[3]

1 E-SAFE COMPLIANCE - TECHNICAL SAFEGUARD

e-Safe Compliance fulfils the requirements of audit control, access control, integrity control and transmission security of EMRs under the technical safeguards requirements of **HIPAA**. The system incorporates classification tools to specify sensitive health data and information, record its usage, and then audit that usage. In addition, e-Safe Compliance has a Rights Management System (RMS) module for data protection using persistent universal encryption to protect sensitive health information in images and documents, and maintaining the integrity of that information. In RMS, encrypted images and documents containing health information have access controls applied to them and the transfer of these images or documents is safeguarded during health information exchanges (HIEs) with other health care entities.

1.1 AUDIT CONTROL

e-Safe Compliance offers an Information Classification Tool which allows information owners, or healthcare providers, to specify sensitive health data even at departmental level (e.g., laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities etc.) and so offers an efficient means of performing data classification. The workflow based on ISO 27001, ensures that all sensitive health related data is classified, the classifications are effective, usage and transfer (via Emails, USB, Clouds, IM etc.) of the classified data is audited, potential incidents are reported and any data leakage incidents that occur are handled appropriately.

Moreover, most of the sensitive health data resides in data stores. e-Safe Compliance, using its discovery tool, scans exchange, databases, SharePoint for health related data or information and once such data is identified, monitoring of this data commences.

1.2 ACCESS & INTEGRITY CONTROLS AND TRANSMISSION SECURITY

e-Safe Compliance RMS uses universal encryption which allows information owners or healthcare providers to protect the images, files or documents containing EMRs. It ensures that the images and documents not only remain encrypted at rest but also remain protected during HIEs over an electronic network, either internally or externally. In addition to that, through persistent encryption RMS ensures the integrity of EMRs and it allows information owners or health care providers to define who can have access to the image or the document using right click options available in the mouse.

Furthermore, in the HIEs, the external health care providers can use (view, edit, print) the protected images or documents by downloading e-Safe Compliance Rights Management iOS/ Android apps from the Apple Store and Google Play Store respectively and install on their mobile devices.

2 CONCLUSION

e-Safe Compliance's subscription based model with R&D as a core, ensures that technical safeguards must evolve as required. On the other hand, a healthcare organisation is much better prepared for numerous types of data breaches if technical safeguards are properly applied in combination with physical and administrative safeguards. In this way, the organisation can keep electronic Protected Health Information (ePHI) from falling into the wrong hands.

3 REFERENCES

1- https://healthitsecurity.com/news/hipaa-administrative-safeguards-basic-review
2- https://healthitsecurity.com/news/hipaa-physical-safeguards-basic-review
3- https://healthitsecurity.com/news/hipaa-technical-safeguards-basic-review