Safe Mail and Safety Chamber - Tool for Exchanging and Storing Encrypted Messages and Files

Rozalija Krstanoska[1], Adrijan Bozinovski[1], Veno Pachovski[1] and Ryszard Janda[2]

[1] School of Computer Science and Information Technology,
University American College Skopje,
1000 Skopje, Macedonia
[2] SCC Soft Computer
Clearwater, Florida

Abstract. No organization is immune to the threat of security breaches, but implementing data encryption is a major safeguard that will protect confidential information and the organization's reputation. Now, a hacker can potentially break into a system remotely and steal patient information. It's an intimidating thought, and when you couple it with HIPAA/HITECH fines that can reach well into the millions, it's easy to miss the days of paper records and locked file cabinets. No organization is immune to the threat of security breaches, but implementing data encryption is a major safeguard that will protect confidential patient information and the organization's reputation. The critical data can be compromised in a number of ways, especially when stored in servers that might change hands over the years. In the case of medical organization, when it is dealing with medical information about the patients, the level of data security must be unquestionable. When considering that detrimental crimes, like e.g. identity theft, are on the rise, data encryption is a must. Safe*Mail* is a unique e-mail solution that enables registered users to exchange encrypted text messages, encrypted screenshots and encrypted attachments to/from any recipient in the world. One message can send up to 10 very large files (up to 3 GB each) with very sensitive contents, and free text containing atoms of confidential data (e.g., financial, personal, etc.). Composing and sending e-mails with Safe*Mail* is permitted only to registered users, initiating the chain of e-mail exchanges. Recipients of these encrypted messages do not need to be registered users to compose responses or forward messages to other recipients. The recipients specified by them in the forward list automatically are granted permission to decrypt messages. Moreover, this tool is supported by another unique and innovative solution called *Safety Chamber* - thetool which assures confidentiality, availability and security of transmitted and stored sensitive data. Safe*Mail* and *Safety Chamber* are intended to send, use, store and view electronic Protected Health Information (ePHI) data, as well as any other types of confidential data.

Keywords: Encryption · Safety · Decryption · E-mail · Chamber · Data token · Context · Data atom · ePH.