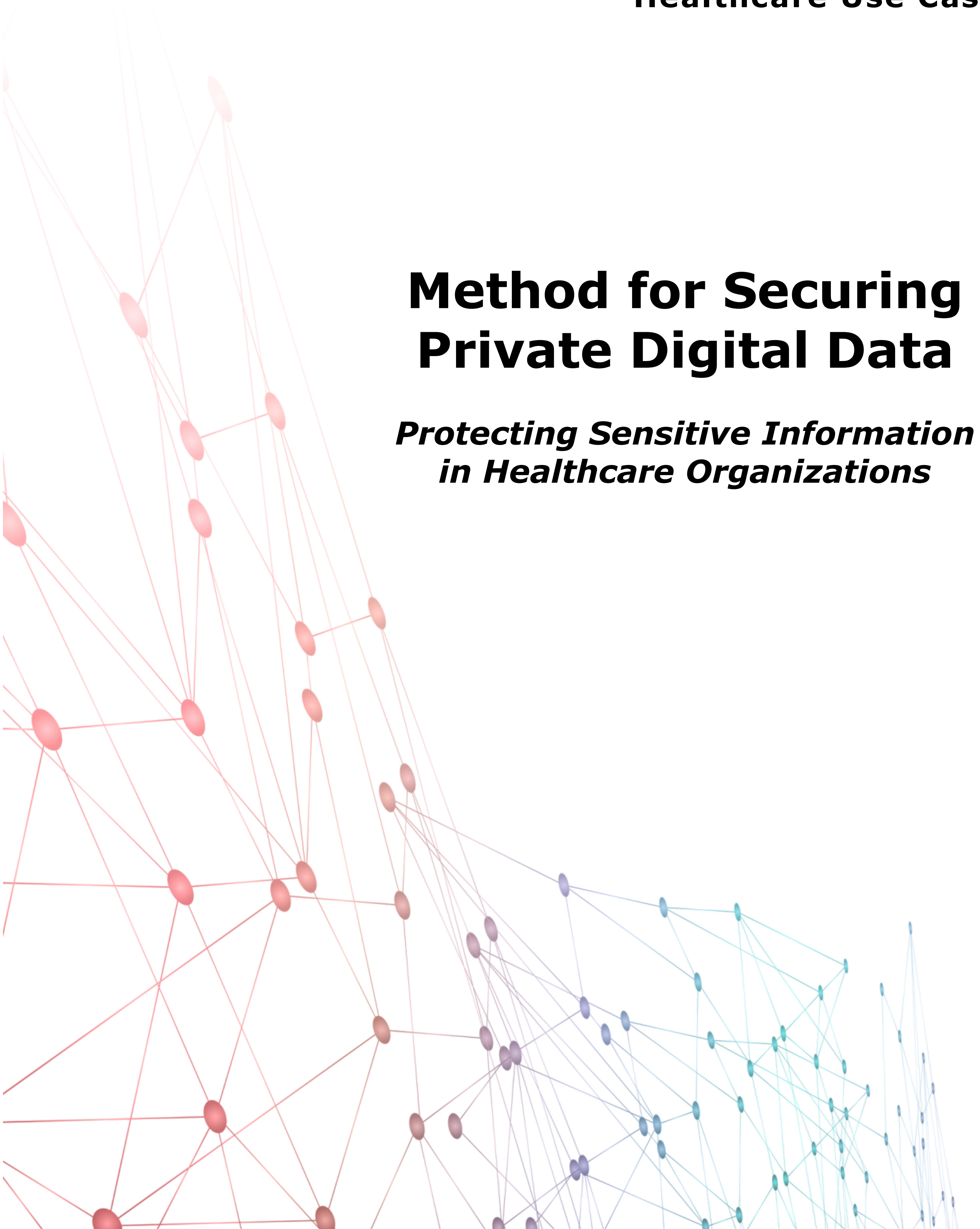
eclypses™

Healthcare Use Case

Method for Securing Private Digital Data

Protecting Sensitive Information in Healthcare Organizations



Introduction

Cybersecurity affects just about everything for everyone in every way for all healthcare providers today. While the first thought of a healthcare organization is to achieve positive outcomes for their patient's condition, there is something just as critical to provide – the security of patient data along with the provider's business files.

Hospitals, clinics, outpatient facilities, private practices, and off premises locations are all vulnerable to attacks. Mass data breaches and cyber-attacks can result in stolen heath and financial records, as well as damage to the healthcare provider's reputation in the community they serve. The risk of fraud and financial loss plus the jeopardy of non-compliance is too great.

Eclypses™ has developed an innovative turnkey data protection solution that keeps all critical data under lock and key, mitigating the risk of a mass data breach. Eclypses' proprietary MicroToken Exchange™ (MTE) data security solutions protect sensitive data from a breach of files and field level data like social security numbers, credit card info, health records, and other sensitive information.

MicroTokenization® replaces data elements with tokens, transforming data into random strings of characters that have no meaningful value to hackers while in motion. When placed into Eclypses' Private Digital Vault storage (data at rest), MicroEncryption® adds another layer of security by encrypting and scattering unrelated segments across multiple hard drives in multiple data centers, to be recalled when needed without affecting the user experience.

Cyber Threat Situation and Protection Objective

The protection of information from cyber intruders is vital within healthcare organizations. Confidential patient information and billing account information are two of the primary targets for cyber-attackers.

The elevated instances of mass cybersecurity breaches through healthcare organizations such as hospitals provides a need for unassailable cybersecurity methods. Private information includes:

- Names
- Birthdays
- Social Security numbers
- Account numbers
- Credit Card numbers
- Insurance information
- Medical records

With the assistance of the dark web, once a bad actor gains access to critical information within databases, it's easy for them to use this data to cause harm.

This use case has been created to provide healthcare organizations with an example of what is continuing to occur with medical mass cyber breaches and how to prevent this. Eclypses' MTE solution provides the security to prevent these breaches from occurring with a level of cybersecurity never before possible because real data is never sent over the Internet or stored on file servers accessible by hackers and fraudsters.

The objective of this use case is to show how a hypothetical healthcare provider, Zenith Hospital, defends against mass data breaches.

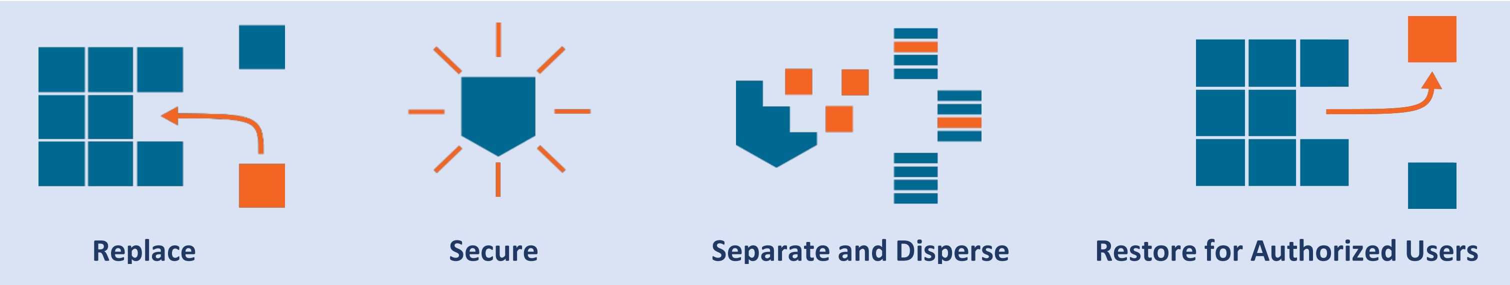
The Approach

Zenith Hospital secures electronic health records, billing information, and other confidential patient data from mass data breaches and cybersecurity attacks through the implementation of Eclypses' MTE solution. MTE improves the reliability of Zenith Hospital's data storage security infrastructure.

By using MicroEncryption processes for data at rest, to provide unusable MicroTokens™ to bad actors during cyber-attacks, confidential patient information stored within databases would be un-useable by bad actors. MicroEncryption creates the ability to facilitate end-to-end security.

The first step in the process is taking a MicroToken and implanting it to replace an individualized data element or elements, down to the field level of a record within a database, or a file, of most any type. Within a database, the non-sensitive data fields would remain in place.

The concept of protecting only that which requires protection is one of the secrets to maintaining millisecond speeds. Once a piece of data is MicroEncrypted, all that would reside is non-sensitive data field elements along with MicroTokens, which are placeholders. MicroTokens do not contain any part or piece of the original sensitive data



For example, a database with 100,000 records, in which 10 sensitive fields were to be protected, would be treated and protected as if it were 1,000,000 individualized databases. With the utilization of MicroEncryption, in the event of a breach, including after an encryption scheme is broken, there is no sensitive data contained within that system to be exploited. That's because it is no longer there and has been moved to the Private Digital Vault.

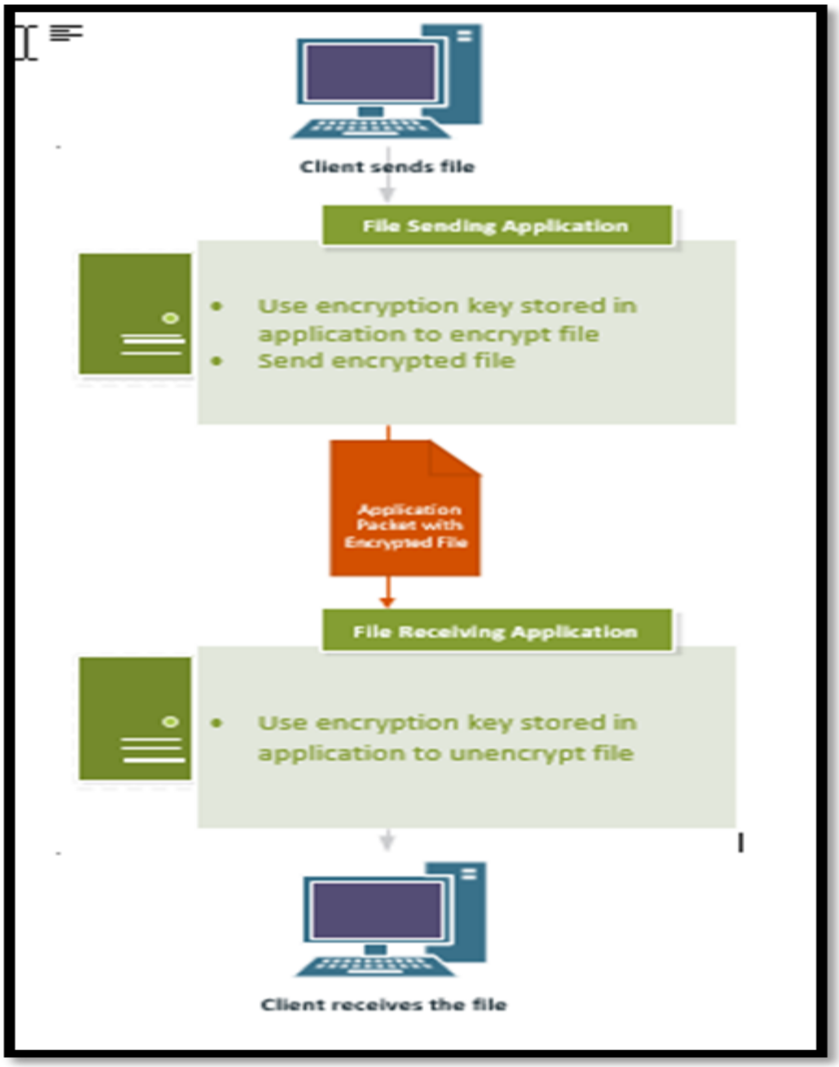
Standard Encryption Versus Eclypses Digital Vault Storage

The following illustrations demonstrate two different scenarios: a typical file transfer application without MTE technology (using standard encryption approaches) and an application built to use the MTE Commander and Digital Vault to safely send files and store them.

Scenario One: File Transfer Application without the MTE Solution

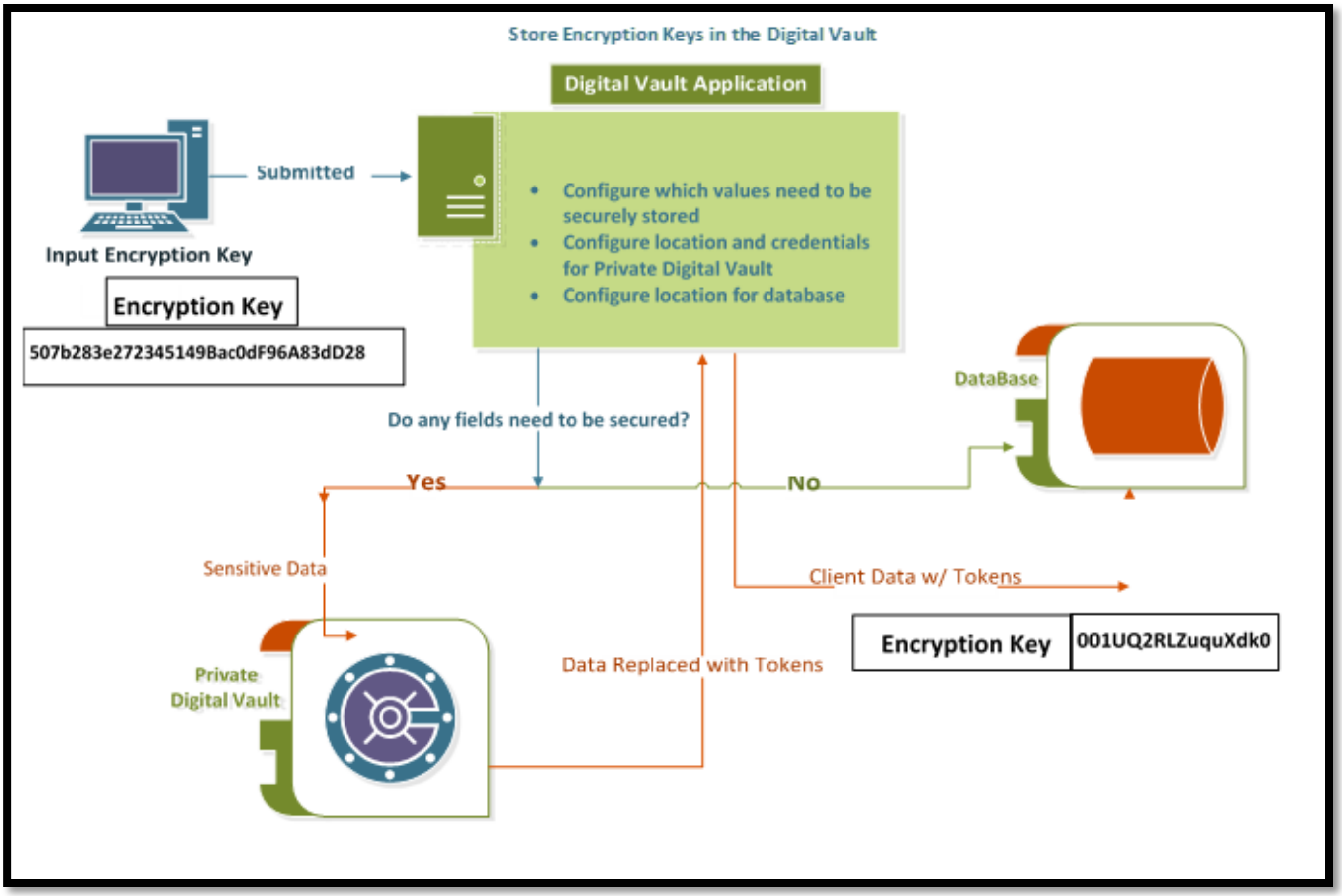
A typical file transfer application typically uses standard encryption methods to protect the file being transferred, such as shown in this diagram.

Encryption keys can be painful to manage and there is the potential that the application may only use one encryption key for all encryption operations. This makes the application and the transferred files vulnerable if the encryption key is detected, allowing hackers into sensitive patient information.


Client sends file
File Sending Application
Use encryption key stored in application to encrypt file
Send encrypted file
Application Packet with Encrypted File
File Receiving Application
Use encryption key stored in application to unencrypt file
Client receives the file

Scenario Two: File Transfer Application with the MTE Solution

An alternative way to handle encryption keys would be to store them in Eclypses' Digital Vault. Instead of having the encryption keys hard coded into the application where the same one is being used over and over, in this scenario the keys are stored in the Digital Vault. That way there are many alternative encryption keys that can be used.


Store Encryption Keys in the Digital Vault
Digital Vault Application
Submitted
Input Encryption Key
Encryption Key
507b283e272345149Bac0dF96A83dD28
• Configure which values need to be securely stored
• Configure location and credentials for Private Digital Vault
• Configure location for database
DataBase
Do any fields need to be secured?
Yes
No
Sensitive Data
Client Data w/ Tokens
Encryption Key
001UQ2RLZuquXdk0
Private Digital Vault
Data Replaced with Tokens

Now the File Transfer application can go to the Digital Vault to select an encryption key. A method can be put in place for the MTE application to randomly select an encryption key by looking at the internal data store that contains the token assigned for the encryption key by the Digital Vault. This keeps confidential patient information hidden and safe from cybercriminals.

If the entire application packet is compromised, the MTE token is instantly obsolete and therefore cannot be used later to retrieve the encryption key from the Digital Vault, providing an additional security layer.

This is the ultimate approach for Zenith Hospital to take to achieve the highest level of cybersecurity protection possible.

About Eclypses

Eclypses' industry leading disruptive cybersecurity software replaces user data with MicroTokens™ using MicroEncryption® to provide the highest level of data privacy available with the company's patent pending MicroToken Exchange™ (MTE) technology.

Applications range from secure command and control needs, including Internet of Things (IoT), to secure storage and retrieval of sensitive data, such as credit card information and healthcare records. Eclypses' MicroToken Exchange technology is helping enterprises and government agencies protect their most sensitive and private information from cybercriminals cyber terrorists today.

Eclypses' MicroToken Exchange (MTE) software complies with the European Union's General Data Protection Regulation (GDPR). In addition, Eclypses' technology is certified as Payment Card Industry Data Security Standard Level 1 (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliant.

The Digital Safety Deposit Box of CertainSafe®, a business unit of Eclypses, has been selected as a 2018 Editors' Choice Product by PC Magazine (PCMag) for best encryption software. In addition, the Digital Safety Deposit Box was designated as the most secure solution tested. The Digital Safety Deposit Box is an ultra-secure cloud-based service that makes it easy for businesses to securely store, access, and share valuable and private assets, and is built on Eclypses' cybersecurity software.

In recapping the coveted award, PCMag's Lead Analyst for Security Neil J. Rubenking writes, "When backing up your sensitive files to the cloud, CertainSafe Digital Safety Deposit Box emphasizes security over all else, but it doesn't sacrifice ease of use." Rubenking added that of all the solutions reviewed, "The Digital Safety Deposit Box has the most secure encryption software."

Located in Colorado Springs, Colorado, you can contact Eclypses at 719-323-6680 or via email at info@eclypses.com. Please visit us at www.eclypses.com and www.certainsafe.com.