Cryptography in Healthcare

Cryptography uses algorithms to create keys that code and secure information by encrypting it as a means of hiding information from unintended users.

Cryptography & Cybersecurity

Cryptography is a form of cybersecurity; it is a technique for protecting information. It involves developing code to encrypt a message like a password, an email, or bank information, etc.

Types of Cryptography

1. Symmetric-key: a single (same) key is used to encrypt & decrypt
2. Asymmetric-key: use a pair of keys, public key is available to anyone, and private key is secret.

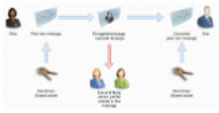
Cryptography in Healthcare

Cryptography is valuable in healthcare because it can be used to encrypt emails that contain confidential health information and to create a secure electronic health record system where information is shared.

Cryptographic Techniques in Healthcare

- Hashing technique is used to ensure integrity; hashing converts plain text to a string of characters that is used to see if data has been tampered with
- Digital signatures are also used to ensure data integrity
- SSL and TLS are used to encrypt information accessed through a web browser and server
- Information in electronic health records are encrypted and can only be accessed with the appropriate key that decrypts the information.

In fact, HIPAA requires that all electronic PHI (protected health information) must be encrypted to protect information from being accessed by unauthorized users. Nullam laoreet sed eros eu viverra. Morbi id venenatis tortor, ultricies venenatis felis.



The Basics of Cryptography

Protects privacy, confidentiality, and authentication, and ensures data integrity and nonrepudiation. Can encrypt and protect sensitive information (like patient information), utilizes digital signatures to verify the integrity of documents, and protects passwords from being deciphered. Simply, cryptography encrypts a message from plain text with a key, and then a key is used to decrypt that mesagge back to plain text.

Cybersecurity in Healthcare

Hospitals and healthcare companies are targets of cyber attacks because of the sensitive and confidential information they store in electronic health record systems. Cryptography can be used to ensure the protection of patient information. Health information also has to abide by HIPAA protocols. Not only is patient privacy important but if HIPAA regulations are not followed, there can be steep legal consequences. Patient data privacy is also becoming more relevant with the rise of telemedicine and remote patient monitoring.

Healthcare Data Breaches

The graph above is from The HIPAA Journal and shows the number of people affected by healthcare security breaches. In 2023, that number was around 140 million. These breaches were often because of a hacking/IT incident, a ransomware attack, or unauthorized disclosure/access.

Conclusion

Cryptography is a cybersecurity tool that is vital in securing information and is especially important in securing sensitive and confidential data including healthcare records and PHI. Cryptography encrypts data so that only authorized users can decrypt and access the data. Cryptography secures stored data and data that is shared or transmitted between users. Cryptography serves a function in protecting electronic health records and the transmission of those records, which is vital in protecting patient privacy and complying with HIPAA regulations.

Made with Infogram

Cryptography in Healthcare

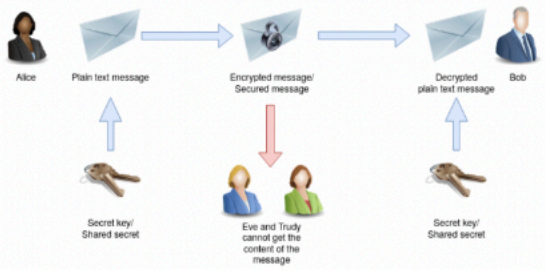
Cryptography uses algorithms to create keys that code and secure information by encrypting it as a means of hiding information from unintended users.

Cryptography & Cybersecurity

Cryptography is a form of cybersecurity; it is a technique for protecting information. It involves developing code to encrypt a message like a password, an email, or bank information, etc.

Types of Cryptography

1. Symmetric-key: a single (same) key is used to encrypt & decrypt
2. Asymmetric-key: use a pair of keys, public key is available to anyone, and private key is secret.



The Basics of Cryptography

Protects privacy, confidentiality, and authentication, and ensures data integrity and nonrepudiation. Can encrypt and protect sensitive information (like patient information), utilizes digital signatures to verify the integrity of documents, and protects passwords from being deciphered. Simply, cryptography encrypts a message from plain text with a key, and then a key is used to decrypt that mesagge back to plain text.

Cryptography in Healthcare

Cryptography is valuable in healthcare because it can be used to encrypt emails that contain confidential health information and to create a secure electronic health record system where information is shared.

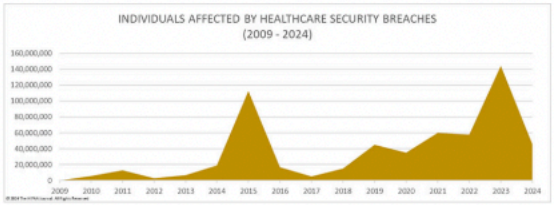
Cybersecurity in Healthcare

Hospitals and healthcare companies are targets of cyber attacks because of the sensitive and confidential information they store in electronic health record systems. Cryptography can be used to ensure the protection of patient information. Health information also has to abide by HIPAA protocols. Not only is patient privacy important but if HIPAA regulations are not followed, there can be steep legal consequences. Patient data privacy is also becoming more relevant with the rise of telemedicine and remote patient monitoring.

Cryptographic Techniques in Healthcare

- Hashing technique is used to ensure integrity; hashing converts plain text to a string of characters that is used to see if data has been tampered with
- Digital signatures are also used to ensure data integrity
- SSL and TLS are used to encrypt information accessed through a web browser and server
- Information in electronic health records are encrypted and can only be accessed with the appropriate key that decrypts the information. In fact, HIPAA requires that all electronic PHI (protected health information) must be encrypted to protect information from being accessed by unauthorized users.

Healthcare Data Breaches



The graph above is from The HIPAA Journal and shows the number of people affected by healthcare security breaches. In 2023, that number was around 140 million. These breaches were often because of a hacking/IT incident, a ransomware attack, or unauthorized disclosure/access.

Conclusion

Cryptography is a cybersecurity tool that is vital in securing information and is especially important in securing sensitive and confidential data including healthcare records and PHI. Cryptography encrypts data so that only authorized users can decrypt and access the data. Cryptography secures stored data and data that is shared or transmitted between users. Cryptography serves a function in protecting electronic health records and the transmission of those records, which is vital in protecting patient privacy and complying with HIPAA regulations.

Share

Made with infogram