CYPHER.DOG®

Cypherdog Encryption

for Healthcare Services

Encrypt any file, any text, and share via any medium, any time

Daily communication within the medical industry is crucial for day to day running of medical facilities and nursing homes working in the healthcare industry, whether it be for long-term care planning, complaint management, or current information regarding the patient's health.

E-mail is a primary method of communication because it is the simplest and quickest means to communicate information constantly and cheaply. The issue that healthcare facilities face is keeping sensitive information confidential. As personal and highly sensitive information is frequently exchanged in the health sector, it is essential to use proper encryption technology to prevent unauthorized access.

The risks associated with unencrypted e-mails in the medical industry

Unencrypted e-mails in the medical industry can pose significant risks to patient privacy and security. When medical professionals use unencrypted e-mail to communicate sensitive patient data, they expose that data to a range of potential security threats. Some of the potential risks associated with unencrypted e-mails in the medical industry include:

- **Data breaches** – Unencrypted e-mails can be easily intercepted and read by hackers or other malicious actors, potentially leading to large-scale data breaches that can compromise the privacy and security of thousands of patients.
- **HIPAA violations** – The Health Insurance Portability and Accountability Act (HIPAA) requires medical professionals to protect patients' private health information (PHI). If medical professionals use unencrypted e-mails to transmit PHI, they may be in violation of HIPAA regulations and face significant legal and financial penalties.
- **Damage to patient trust** – Patients expect that their personal health information will be kept confidential and secure. If a medical business or organization experiences a data breach or other security incident because of unencrypted e-mails, patients may lose trust in that organization and seek care elsewhere.

How encryption software can help protect sensitive data in the medical industry

Encryption software can help protect sensitive data in the medical industry by providing a secure method for transmitting confidential information. Cypherdog Encryption uses advanced encryption methods to protect the content of e-mails and other electronic communications from unauthorized access. Additionally, our software includes a range of security features, such as two-factor authentication and data loss prevention tools, to further enhance the security of users' data.

By using our encryption software, medical professionals can ensure that patient data is kept confidential and secure, reducing the risk of data breaches and HIPAA violations. Our software also helps to protect patient trust by providing a secure method for communicating sensitive information.

Benefits of using encryption in the medical industry

The benefits of using encryption in the medical industry are numerous. By using Cypherdog Encryption software, medical businesses and organizations can enjoy benefits such as:

- **Secure Communication** – E-mail encryption software can provide a secure means of communication between healthcare providers, patients, and other parties involved in the medical industry. This can help prevent data breaches and protect sensitive information from being intercepted by unauthorized third parties.
- **Compliance with regulations** – HIPAA requires medical professionals to protect patient's private health information (PHI). By using encryption software, medical professionals can ensure that they are following HIPAA regulations.
- **Data Integrity** – Encryption software can also help ensure the integrity of data by preventing unauthorized changes to the content of an e-mail message. This is important in healthcare settings, where even small errors or changes to patient data can have significant consequences.
- **Improved patient trust** – Patients expect that their personal health information will be kept confidential and secure. By using encryption software, medical businesses and organizations can demonstrate their commitment to protecting patient privacy and security, building trust with patients, and improving patient satisfaction.

Implementing encryption in the medical industry

Implementing encryption in the medical industry can be a complex process, but Cypherdog Encryption software makes it easy. To implement an encryption solution, medical businesses and organizations should:

- **Choose the right software** – Our sophisticated encryption software for the medical industry provides robust security features and compliance with HIPAA regulations.
- **Train staff** – Medical professionals should be trained on how to use an encryption software properly to ensure that patient data remains secure.
- **Establish best practices** – Medical businesses and organizations should establish best practices for using encryption, including guidelines for how and when to use it and policies for reporting security incidents.

What type of data does your organization process?

1. You store and exchange documents and e-mails containing sensitive data such as patient documents, results of diagnostic tests, medical cards, and treatment history. You exchange documents and e-mails internally and often send patient documents outside your organization.
2. You send and store documents with sensitive intellectual property information that pharmaceutical companies should protect.
3. You exchange documents with law firms, HR agencies, external accounting offices, auditors, banks, insurance brokers, marketing agencies, and others.

Why should you protect yourself and your patients?

1. Avoid data leaks - when everybody could know about your patients' sensitive documents.
2. Avoid ransomware with double extortion when data from your notebooks, e-mail, and servers gets stolen, and you are blackmailed and forced to pay a ransom. Hackers demand a ransom for not disclosing stolen data but might do it anyway.
3. Avoid corporate espionage - especially in the the pharma sector.
4. Avoid invoice or other documentation hacking - when your customer paid using the wrong wire transfer information based on a fake invoice.

What can happen after a cybersecurity incident?

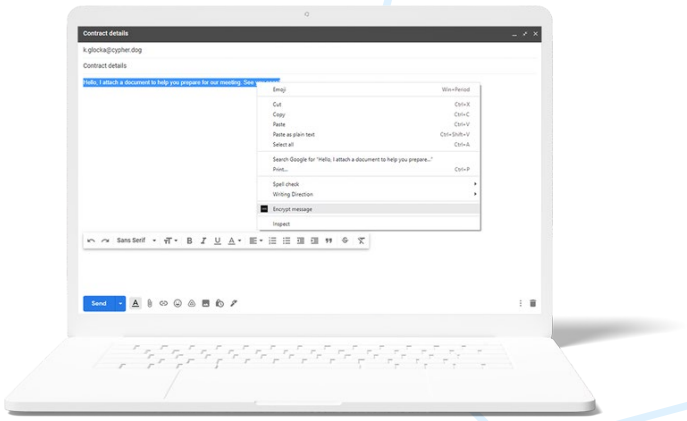
1. You might have to pay financial penalties to the regulators (GDPR, DORA, NIS-2, Privacy Acts, and others).
2. You can lose the trust of your patients after a data leak. Sometimes, you should expect a case to be filed against you.
3. You could have to pay a ransom to hackers because continuity of operations is crucial in the healthcare sector, and you cannot function with the lives and health of your patients in mind.
4. You can damage your reputation as a doctor, which could be detrimental to your business.

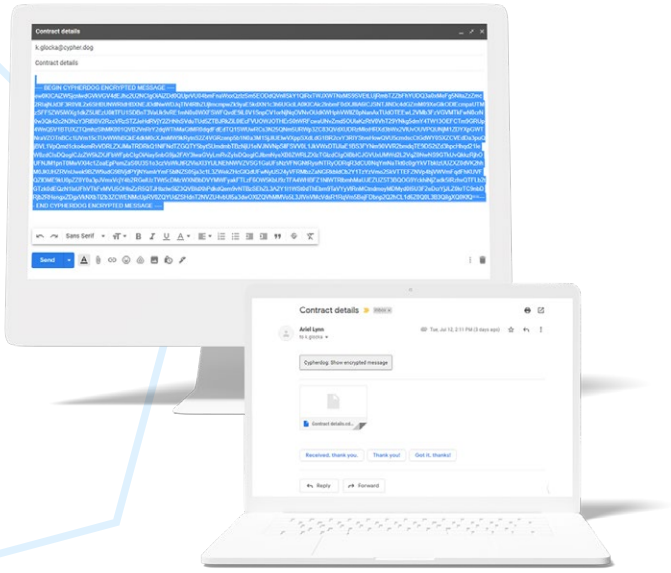
How it works

One-click. Complete protection. Cypherdog Encryption allows you to encrypt and decrypt any text or file and send them using any media, including e-mails supported by plugins to **Firefox, Chrome and Edge browsers, Gmail/Google Suite, Addins in Outlook and Thunderbird.**

You can send and receive encrypted files and messages using any web client or native e-mail client or Slack, WeTransfer, Google Drive, or any other communication method.

You are always assured that only the authorized recipient will have access to the decrypted content.





Threats in cyberspace

E-mail is one of the most popular electronic communication channels. Like most digital services, it is vulnerable to cyberattacks, which may result in **unwanted access** to your mailbox and **disclosure of confidential information**. In the event of unauthorized use of the compromised e-mail box, message recipients cannot verify the sender's identity.

Cypherdog is a **comprehensive solution** to both threats. On the one hand, it ensures message encryption (hiding the content from unauthorized users); on the other hand, it allows the recipient to verify the sender's identity.

We protect you against

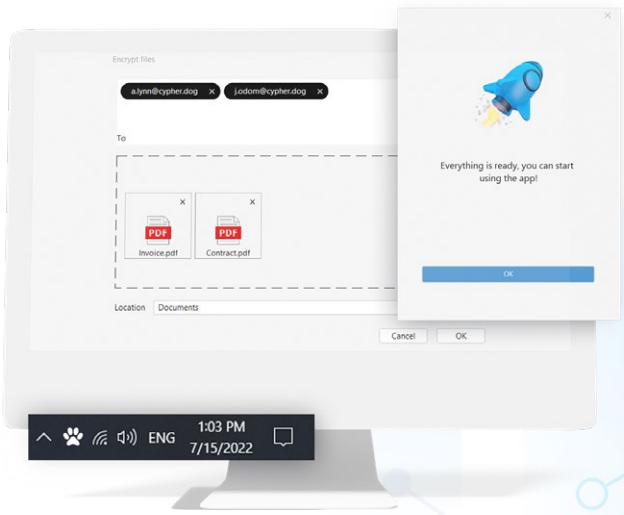
- corporate espionage
- data leaks
- new generation of ransomware with double extorsion
- invoice hacking
- business e-mail compromise (#BEC)

We support you in becoming compliant with GDPR, Privacy Acts, DORA-2, NIS-2, and ISO 2700x implementations, among other regulations.

Friendly user interface

Cypherdog software focuses on simplicity and ease of use. During installation, the program will ask for the **password to your private key** and will allow you to **make a backup** of it (use a USB drive or print a copy of the key on a piece of paper, in the Business version backup is made automatically on company's server). After the installation is complete, **you can encrypt messages and send them via your e-mail immediately.**

macOS



Asymmetric encryption

Absolute protection of private key

No "trusted" third party

Zero-knowledge security model

No service provider access to data

Lack of metadata & logs

Identity trust methods

Cypherdog Encryption specifications	Free (after Trial)	Single User & Trial	Business
Text/e-mail messages encryption	-	x	x
Encryption of files/attachments in e-mail messages	-	x	x
Decryption of e-mail messages/ texts and attachments/ files	x	x	x
Administration panel for users & private keys management	-	-	x
Backup private key to file (on device)	x	x	-
Backup of private key to company server in Vault	-	-	x
One license for a single user	x	x	-
One license for multiple users	-	-	x
Basic support and online training	x	x	-
Advanced support and training	-	-	x
E-mail aliases	x	x	-
Cryptography	Encryption: asymmetric RSA3072 and symmetric AES-256, SHA512 hash function		
Microsoft Outlook	Add-ins to Outlook 2016+ for Microsoft 365/ Exchange Server, webclient & native		
Gmail & Google Suite	Plugins: Google Chrome, Microsoft Edge, Mozilla Firefox		
Mozilla Thunderbird	Add-ons for Thunderbird for all e-mail providers and servers		
Other e-mail clients	Manual encryption / decryption / right-click or "magic window"		
Other communication channels	WeTransfer, Slack, Google Drive, Dropbox, WhatsApp, Messenger etc.		
Operating systems	Windows, macOS, Linux		

CYPHER.DOG®

Cypherdog Security Inc., 100 Wilshire Blvd., Suite 700, Santa Monica, 90401 CA, USA
www.cypher.dog | info@cypher.dog