

# The Guide to Protecting **Data in Motion**

# CONTENTS

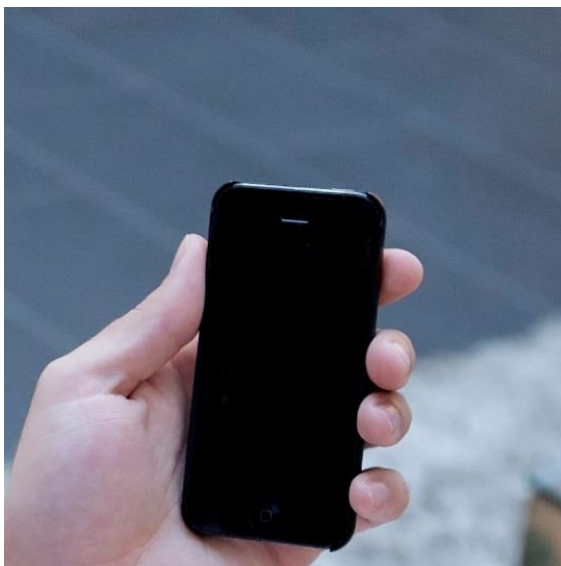
| Chapter          | Contents  | Page |
|------------------|---|------|
| <b>Chapter 1</b> | The three states of data – data at rest, in use and in motion | 3    |
| <b>Chapter 2</b> | Why data in motion is particularly vulnerable                 | 4    |
| <b>Chapter 3</b> | The evolving nature and use of data in motion                 | 5    |
| <b>Chapter 4</b> | Regulations impacting data in motion                          | 7    |
| <b>Chapter 5</b> | Critical elements for securing data in motion                 | 12   |
| <b>Chapter 6</b> | Finding the right solution                                    | 15   |
| <b>Chapter 7</b> | Why it pays to protect data in motion                         | 19   |

# THE THREE STATES OF DATA

## Data at Rest, in Use and in Motion

In today's digitally-driven world, data is often an enterprise's biggest and most important asset. There are many different types of data, and some of it is sensitive and needs to be protected. Understanding the three different states of data (at rest, in use, and in motion) will help you keep information secure and protected from cyber threats.

Data that needs to be protected exists in three states: at rest, in use and in motion.



Wikipedia defines these three states as:

**“Data at rest:** inactive data that is stored physically in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).”

**“Data in use:** active data which is stored in a non-persistent digital state typically in computer random-access memory (RAM), CPU caches, or CPU registers.”

**“Data in motion:** information that flows over the public or untrusted network such as the internet and data which flows in the confines of a private network such as a corporate or enterprise Local Area Network (LAN).”

Data in each state is vulnerable in different ways, and as such require different techniques and tools for securing it. While it is important to secure data in all its modes, data in motion is particularly vulnerable and requires specialized capabilities.

There are numerous ways to move or send data. A growing volume of sensitive data is being transmitted digitally with email being the most common. These range from individual emails sent one at a time to legacy applications generating thousands of automated messages simultaneously – and often with file attachments – to messaging capabilities integrated with online applications and portals. Texting, chat and online file exchange services are some other examples of data in motion.

# WHY DATA IN MOTION

## is Particularly Vulnerable

When an email or anything else is sent over an unsecured network – i.e. the internet, it typically takes many internet ‘hops’ across the labyrinth of public servers and broadband pipes that make up the virtual fabric of the public internet.

Anyone with the right tools can intercept an email as it moves along this path. Using a standard email service or unsecured website to send or exchange sensitive or confidential information, either online, in the plain-text body of the email, or as an attachment, is like writing that information on the back of a postcard. Like a postcard, anyone handling or intercepting unprotected data along its electronic journey to the intended recipient can easily read it.

This is because the three primary protocols used to send and receive email are vulnerable to eavesdropping. Simple Mail Transport Protocol (SMTP), the worldwide standard for email transmission, is typically implemented without [encryption](#). Likewise, Post Office Protocol (POP) and Internet Message Access Protocol (IMAP), the two standards for retrieving email from remote servers, are also typically implemented without encryption. When not protected, every email message sent via SMTP, POP and IMAP protocols can be viewed by anyone with a PC, an internet connection and a network sniffer. The same goes for files and other data exchanged online on unprotected sites.

It’s a surprising truth that although email is the most widely used form of business communication in the world, it’s also the least secure. Users and businesses routinely exchange sensitive and confidential information such as passwords, credit card data and health information through email. This should be a significant concern for any business seeking to protect the sensitive information of their customers, safeguard confidential communications with business partners, and comply with state and federal privacy regulations. Fortunately, encryption technology has progressed to a point that email is now the easiest form of communication for organizations to secure.

*“Combining simplicity with security is a key component for organizations that need to protect their sensitive data and maintain compliance with industry regulations.”*

**Bob Janacek, CEO, DataMotion**

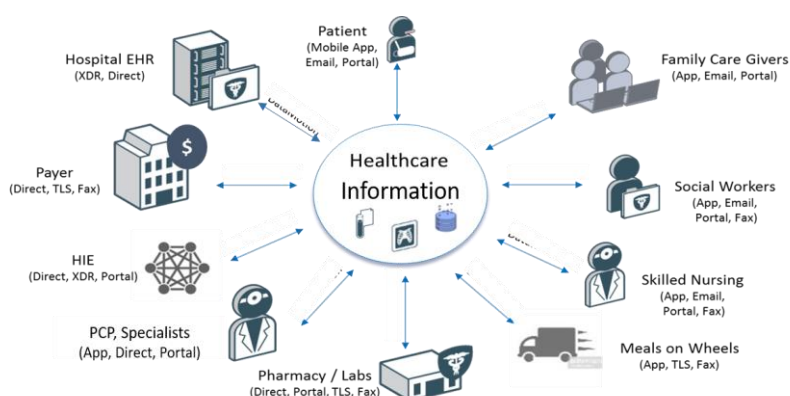


# THE EVOLVING NATURE

## and use of Data in Motion

The amount of data flowing in and out of an organization's internal network is growing in volume and in how it is being used. Today's expectation of immediacy dictates that increased amounts of sensitive data be transmitted digitally— forcing many organizations to replace couriers, faxes and conventional mail service with faster options such as email, chat and online file exchange.

For example, more than 124 billion messages flow through business email accounts each day, and that number is projected to increase to more than 128 billion by 2019. And over 95% of the data payload is in file attachments.<sup>1</sup> The use of email is so ubiquitous that office workers and managers spend as much as a third of their day just reading and answering emails. Other forms of communicating and sending messages digitally are also increasing in usage, such as texting, chat and online file exchange.



### The changing nature of health data exchange workflows

The use of data in motion has and continues to evolve, as have the methods for securing it. Three trends are emerging here. One is the [integration of encryption into common business workflows](#) with the organizational goal of simplifying and enhancing both the workflow, as well as the security and compliance experience – all with little to no impact on expenses.

This integration is driven equally by the need to comply with regulations and the desire to use more efficient digital workflows to send sensitive data in a way that is easy for the user and the organization. This means seamless integration into mobile applications, CRMs, contact centers and of course messaging applications and file sharing processes. A good example of this is found in healthcare. Data exchange patterns are shifting from primarily intra-enterprise, to external entities like EHR and email platforms CRM, mobile and contact centers.

A second and perhaps bigger trend is the simplification of the customer/client experience, which is manifesting in multiple ways. More and more organizations are utilizing TLS encryption because it simplifies the end-user experience by masking the fact that the messages received were encrypted. The messages appear in their inbox just like any other email, encrypted and ready to read. The customer can reply and have their message encrypted – and not even realize that their communications were automatically protected.

<sup>1</sup> The Radicati Group, Inc., "Email Statistics Report, 2015-2019," 2015.

<sup>2</sup> Carleton University, "Carleton Study Finds People Spending a Third of Job Time on Emails," 2017.



## Simplifying the Customer Experience

*A secure message center adds encrypted web-mail, web-form or web-chat services natively to financial services customer portals and mobile apps so that clients can easily ask questions about their account and even share supporting files or images (receipts for a credit charge dispute, a tax return as part of a loan application process). Client messages and files are routed to responsible employees – account teams, support personnel, or contact center agents for a response. Case numbers may be assigned for tracking in ticketing systems and response notifications are sent via email or SMS text channels to notify customers of a waiting reply. For security and regulatory compliance reasons, the message content (and any uploaded file or image attachments) must use encryption for security. Detailed logging and tracking reports provide history and proof for compliance audits.*

Another example is the consolidation of all forms of messaging with a client or customer – including secure methods – in a CRM, customer portal or contact center. Traditionally secure methods of communicating with clients have had to be done in a separate secure portal or tool, making it more challenging to see the overall ‘picture’ of a customer’s communications with the organization. And for the client – frustrating to know where to go and what to send. In addition, organizations are starting to give the customer/client the ability to initiate a secure exchange. The consolidation of these capabilities in one portal or contact center simplifies the “end user” or client experience a great deal, with happier clients as the end result.

A third trend that is starting to emerge is the integration of encryption into business workflows primarily to make the workflow more efficient and effective. Although meeting compliance and privacy regulations is a necessary component of securing data in motion, it is not the primary driver for these kinds of digital transformation.

# REGULATIONS IMPACTING

## Data in Motion

Since the 1990s, the laws impacting data security have evolved and grown. Originally focused on primary data holders, these laws have been extended in recent years to apply to thousands of additional organizations that are business associates of the primary data holders. Under some of these laws, if a business interacts with companies that collect, store or otherwise process individuals' personal information—whether it's credit card numbers or medical lab work—that business may be required to exhibit the same level of care with regards to the security of that information as the companies that collect it. This means an organization may need to be PCI or HIPAA-compliant, even if they don't process financial data or provide medical care.



Compliance violations can put an organization, its customers and clients at serious risk. A primary source of risk exposure is data in motion – such as email. There are at least [four major regulations](#) that have significance for the protection of data in motion.

- ✓ Payment Card Industry Data Security Standard (PCI DSS)
- ✓ Health Information Portability and Accountability Act (HIPAA/HITECH)
- ✓ Gramm-Leach-Bliley Act (GLBA)
- ✓ General Data Protection Regulation (GDPR)

# PCI DSS

## Payment Card Industry Data Security Standard

PCI regulates the security of credit card information stored, processed or transmitted by merchants and associated vendors. [Requirement number 4](#) says that cardholder data passing over an open, public network such as the internet, must be protected (encrypted).

Though PCI is an industry regulation, there are laws at both the state and federal level that effectively force PCI compliance. Therefore, any business that uses credit card information should have PCI on its radar. This includes many kinds of organizations ranging from financial institutions to e-commerce software vendors to online data hosting companies and more. PCI DSS helps organizations focus on security, not compliance, by making payment security business-as-usual. By raising security standards and making compliance status quo, monitoring the effectiveness of security controls and maintaining a PCI DSS compliant environment is much easier.

All credit card processors have adopted the PCI-DSS. The goal of this regulation is to prevent identity theft and protect cardholder data and it applies to any company that processes credit card data. The most recent version of PCI (3.2) was released in April 2016 with a [minor update \(3.2.1\)](#) issued in July 2018 to update migration dates.

PCI-DSS 3.2 mainly consists of changes meant to streamline and clarify the regulation, but there are a few updates that fall under the “evolving requirement” category that affects how you handle credit card data as of February 1, 2018.

An example of a larger change is that there is a [“new requirement for service providers to maintain a documented description of the cryptographic architecture.”](#) Although more documentation is required to stay compliant with the new PCI-DSS update, the goal continues to be ensuring safer communications between business processes and protecting sensitive client information. This update is also expected to help companies detect bottlenecks in their cryptography functionality, giving them an opportunity to make appropriate changes.

A more detailed description of the updates can be found [here](#).

# 20.8%

companies assessed after a data breach were not in compliance with Requirement 4<sup>3</sup>

*There is a clear link between PCI DSS compliance and an organization's ability to defend itself against cyberattacks.*

—[Verizon](#)

3 Verizon Inc. “Verizon 2017 Payment Security Report.” August 2017.



# HIPAA/HITECH

## Health Information Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act

Congress passed HIPAA in 1996. [The HIPAA Security Rule](#), which sets standards for patient data security, and the [HIPAA Privacy Rule](#), also called the Standards for Privacy of Individually Identifiable Health Information, are particularly relevant to securing data in transit. HIPAA provided the first nationally recognized regulation for the use/disclosure of an individual's health information. Essentially, HIPAA defines how organizations impacted by it, called “covered entities”, can use individually identifiable health information or PHI (Protected Health Information).

### Key HIPAA impacts on data in motion:

- *Organizations must ensure email messages and other moving data containing protected health information are sent protected.*
- *Senders and recipients are properly verified and authenticated.*
- *Email servers and the messages they contain are protected.*



Since 1996 HIPAA has been significantly strengthened. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was passed to promote the “[adoption and meaningful use of health information technology](#)”. In HITECH, Subtitle D addresses “[the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules](#)”. HIPAA/HITECH was expanded with the addition of the [Omnibus Rule](#), which became effective September 2013. This rule essentially gave HIPAA/HITECH teeth in compliance and enforcement. The rule significantly increased the number and type of organizations covered by redefining who is considered a business associate of covered entities.

Anyone exposed to patient information—be they labs, third-party billing companies, even janitorial service companies and software services companies—could qualify as business associates (BA) under HITECH and therefore be subject to the same standard of privacy and security as the medical provider they service.

HIPAA now effectively applies not just to medical providers, but to the entire ecosystem of vendors supporting them. Subcontractors who have access to or who store PHI now also need to sign business associate agreements and be in a position to demonstrate compliance.

Business associate agreements (BAA), are contracts that are required to be established between a HIPAA-covered entity and a HIPAA business associate. This contract protects PHI in accordance with HIPAA guidelines. Under the HITECH Act, business associates are responsible for securely handling PHI and can be held accountable and penalized for noncompliance. Therefore, these businesses must also take steps to protect PHI.

# GLBA

## Gramm-Leach-Bliley Act

GLBA was passed in 1999 with primary goal of protecting the private financial data of consumers. This law requires financial institutions to publish and follow a privacy policy, which they supply to their customers upon first purchase/use of service and annually thereafter (or whenever it changes). These are the notices that come from credit card providers on a regular basis. They are also seen when signing up on certain websites. Any business that provides any kind of financial service—from bankers, to insurance agents or companies that provide investment advice—are subject to this law.

- ✓ The Financial Privacy Rule is the key consideration for most organizations. This rule governs the collection, use, and disclosure of private financial data. The process companies must take to safeguard this information is also defined.
- ✓ The Safeguards Rule instructs companies to develop security programs in alignment with the amount of nonpublic information (NPI) data they maintain.
- ✓ Although the law is technology neutral, the Safeguards Rule instructs organizations to implement policies to encrypt or block email traffic based on the message sender, recipient or content.



**According to the Federal Trade commission organizations should** “Take steps to ensure the secure transmission of customer information. For example:

- When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
- If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
- If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.”

*Federal Trade Commission. “[Complying with the Safeguards Rule.](#)”*

# GDPR

## General Data Protection Regulation

### Article 5.1

#### General Data Protection Regulation

*“(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);*  
*(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);*  
*(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);*  
*(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);*  
*(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);*  
*(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”*

GDPR is a new major privacy regulation that went into effect in May 2018. Though it is a European Union (EU) directive it still impacts organizations outside of the EU if those organizations market to and collect information on EU residents. Article 5 of the GDPR details the principles covered by the regulation and 5.1 lays out the requirements for treating the private data of EU citizens.



Essentially this means when collecting, processing and/or storing the personal data of any EU resident – regardless of where the organization is located – express permission must be obtained first. This means the individual must have opted in, not only to collect the data, but to process and store it. Data collectors/processors must also be clear about how the data will be used, stored and protected. Also, these individuals must be given an easy way to withdraw their consent and have it fully deleted from an organization’s database(s). [You can learn more about GDPR here.](#)

A major facet of meeting the requirements of all these compliance policies is ensuring that data in motion is secure and well protected against hackers, scammers and those with the intent of committing fraud.

# CRITICAL ELEMENTS FOR

## Securing Data in Motion

Encryption technology has been around for a long time and is essential for securing data in motion. In essence, encryption is a set of algorithms that protect electronic data from being intercepted and viewed by unintended recipients. How it works is less important than how it's implemented. In fact, many of the most important elements have nothing to do with the technology itself. Here are three critical elements for [developing a plan to secure data in motion](#).

### 1. Start with Assembling a Team

Securing data in motion isn't the job of just one person. Be sure to include all necessary positions and departments from the beginning. To determine who in an organization should be a part of these discussions ask these questions:



- ✓ Who in the organization 'touches' the data we need to secure on a regular basis?
- ✓ Who can lend valuable knowledge about defining our policies?
- ✓ Who would be responsible for enforcing our policies?
- ✓ Who has the technical skills need for selecting and implementing a solution?

Involving everyone up-front means less backtracking and unnecessary changes down the road. Be sure to consider people from legal, compliance, HR, IT and marketing departments. Marketers can help translate policies into layman's terms for your end-users and help "sell" them on policy compliance.

## 2. Conduct an Information Risk Assessment

The security needs of every organization vary. Unless an organization has recently conducted a holistic risk assessment, the threat of a data breach is probably much larger and more immediate than realized. Organizations often underestimate their risk because they erroneously believe all their sensitive data is contained within a few secure systems. In reality, this is seldom true.

Examine all business processes that involve moving data. Think about the situation from a workflow perspective. Do employees access corporate systems from their personal devices or use company-issued devices to work from home? What happens when employees take their devices on business trips? How is data transferred between devices or communicated to other stakeholders? What do customers or business partners do with any sensitive files sent to them? Before moving anything, understand and know where sensitive data resides, who needs to share it and with whom they need to share it. Especially take a good look at what third-party users exchange with, including inbound workflows. Find out what file sharing services are often used and what their potential risks are. Get a good understanding of how this data will flow. After determining how a company transmits information such as credit card numbers, personally-identifiable information and health records, organizations can begin to formulate a plan for how to safeguard that information during transit.



### Risk Assessment Question Checklist

- *What types of sensitive data does your organization store, use, or transmit?*
- *Who has access to this data?*
- *Where, when, and why are they using it?*
- *How is data stored when it is not in use?*
- *How is access to databases controlled?*
- *What mechanisms are used to transport data?*
- *What are the pertinent laws, regulations, and standards?*

## 3. Complete a Policy Review

The third step is to complete a policy review, update existing policies and develop new ones that are needed. There are six recommendations for completing a policy review (a thru f below).

**a. Understand what is driving security policy for data in motion.** Implementing effective policies requires knowing what factors, internal and external, are driving the need to secure data. Some industries and businesses are more heavily impacted than others by government and industry regulations like [HIPAA](#), PCI, GLBA and FERPA. Healthcare entities and financial services organizations are examples of industries strongly impacted by government regulations. Get a clear understanding of the regulations an organization must abide by when transferring sensitive data. Another driver for developing security policies is to protect the organization from a cyber-attack or security breach. Besides being costly, data breaches often cause major damage to the organization's reputation with a corresponding hit on revenue. It's important here to understand the organization's tolerance to this risk. Organizations like investment advisors, medical care providers, legal services and high-tech development may have less tolerance for risking a breach. Other organizations may be willing to take on more risk in order to facilitate conducting business. What is needed is to understand where an organization falls on this risk tolerance line. A third driver is the desire for greater efficiencies in business workflows. Security has been a hindrance to conducting business, and employees will find ways around it because it is too difficult. Some organizations are now driven by a need to transform old workflows that are "too hard" into something more efficient, easy to use and also secure and compliant.



**b. Identify the data.** Identify and understand what data needs to stay private and why. This step will be driven by the reasons that were outlined for needing policies, discussed in the previous section. Some data sets, like social security numbers, are obviously sensitive and apply to most organizations. Other sensitive data may be specific to the organization, such as an account number or an entire department whose communications need to be protected and encrypted. This is why a team is needed.

**c. Forget about patterns. Match sensitive data exactly.** Whenever policy filters are commonly used to secure data in motion, the filters search for patterns in outbound messages and secure the content when those patterns are found. The problem with this functionality is that one keystroke can unbreak a pattern and then private information gets sent unsecured. Work to [match actual data sets](#) and not a pattern of what the data should look like. For example, a pattern may be that an account number has 2 letters followed by 6 numbers. But instead of writing a pattern match to search, set filter to look explicitly for the exact account numbers in the messages.

**d. Know the user.** In order to ensure that outbound email security policy is adhered to, there needs to be an understanding of the end-user experience - know who end users are. This can have a huge impact on

whether or not policies are followed. To keep it simple, make sure policies integrate and work within existing business processes. If users must change their behavior too much to add security, they have a harder time getting their job done and are then resistant (and resentful) about the change.

**e. Combine protection and policy.** Whenever possible, try to layer protection in the policy creation. For example, providing users a way to explicitly mark an outgoing message to be sent securely benefits the message load (those tend to be very quick filter checks) and also by providing a first pass security checkpoint. Users can serve as the first step to identify what outgoing data needs security. Often times they know that some data should be sent securely even if it doesn't conform to filtering rules. This increases the success rate of sending the right data securely by combining user knowledge and company policy.

**f. Remember to keep it simple.** Regardless of how bulletproof data in motion security policy is, rules won't be followed if they are too complex. For maximum policy compliance, keep policies clear and concise. To make sure they are understood, start by outlining and communicating why the policies exist and what the dangers and risks are if they are not followed. Also, be sure the policies adhere to business processes and do not interrupt the daily flow of work for end users.


# FINDING THE RIGHT SOLUTION

## Eight Elements to Look For

The best way to ensure that your messages and attachments remain confidential is to transmit them through an encryption platform that integrates with existing systems and workflows. Optimally, users should be able to send and receive encrypted messages directly from their standard email service. Policy filters that automatically detect sensitive information in email and attached files can automate the encryption process to further ensure security (and regulatory compliance). There are eight key elements to look for in a solution.

### 1. Ease of Use

Look for solutions that are [simple and easy to use for users and recipients](#), without a lot of extra steps, even when sent outside your network. Ease of use is directly related to user compliance. The harder it is and more steps that need to be taken, the less likely they will comply and use it.



**Ask yourself these questions:**

- Can messages and files be delivered directly to a recipient's inbox, decrypted and ready to read, such as through a SmartTLS function?
- Does the solution follow a natural intuitive workflow?
- Does the solution work in conjunction with already used tools, such as Outlook?
- Can recipients easily respond, without the need to install anything?

When it comes to user and recipient ease of use, transparency and simplicity are key elements. Today's modern and evolved encryption solutions can do the complex work of encrypting, decrypting, managing keys, delivery and tracking in the background, making usage seamless.



## 2. Policy-based Filtering

Automated, policy-based filtering reduces the need for user action, working transparently behind the scenes to protect data in motion. Verify the solution uses policy-based filtering to check all email, file attachments and other messages for sensitive, regulated information. Make sure to deploy technology that can filter messages and the wide variety of file format attachments used in business today. To avoid false-positives and an ensuing drain on IT hours and resources, use technology that is designed to minimize false positives yet catch data that cannot leave the company in an unencrypted state.

*The ability to customize email filtering has virtually eliminated false positives, and it's easy to update and change the filtering rules.*

*—Stillwater Medical Center*

### Stillwater Medical Center

*Automatic email encryption for PHI*

This case study from Stillwater Medical Center, highlights the value of implementing an email policy gateway as part of an overall HIPAA data loss prevention policy. Stillwater used a manual and automatic email encryption process to help ensure HIPAA email compliance and data loss prevention for the medical center – with great success!







### 3. On-Premises or Cloud

While cloud-based data in motion encryption solutions are easy to deploy and use, many organizations need the enhanced security and control of an on-premises solution. For some law enforcement applications, CJIS rules will dictate on-premises deployment in a CJIS data center. Make sure the provider offers the flexibility to do both.

### 4. Bi-directional Encryption

Customers and clients – normally the recipients – are starting to demand the ability to send sensitive data to the organizations they buy from, and they want these communications protected as well. Be sure the provider [can secure incoming and outgoing sensitive data](#), such as that directed to a customer service agent.

### 5. End-to-End Security

The solution should provide end-to-end security and multiple delivery methods. Many solutions, including Office 365 utilize TLS, but [not all TLS implementations](#) are the same and not all recipient organizations are enabled to receive email via TLS. To ensure compliance, be sure your implementation covers those situations where TLS can't be used. Multiple delivery options that happen automatically when one path is not secure is ideal.

### 6 Ways Customers Want to Use Customer / Client Portals to Exchange Information

1. *Using any device, anytime, anywhere*
2. *Uploading sensitive documents to client portal*
3. *Clicking an upload link in an email sent by an agent during a conversation on the phone*
4. *Sending a message through the publicly available customer message link on the website*
5. *By sending an email to the publicly available support email address*
6. *Responding to an email sent by an agent / company representative a long time ago.*



### **Government Funded Consumer Complaint Agency**

*This case study discusses how a national government agency used email encryption APIs to bridge legacy systems workflows securely while keeping costs in budget. The agency estimates they received \$5 in value for every \$1 spent on their solution. The agency's mission is to help citizens resolve disagreements with suppliers of goods or services. They process over a million consumer complaint cases per year via the agency's website and call center, with many containing confidential and personally identifiable information. The cases need to be transmitted securely to local and federal authorities as well as trading partners and need very rapid resolution. The information interacts with disparate computing environments both internally and with external partners.*

## **6. Has Your Back**

Delivery of a full range of support options is a must. Large enterprises in particular often have complex systems, infrastructure and custom needs. Availability of basic support through full service 24/7 engagements can make the implementation process much smoother.

## **7. Road Protection**

With today's more mobile workforce, employees conduct a great deal of business outside of the office. Look for a solution that is optimized for mobile devices and works with existing email clients on mobile devices so no separate app is needed.

## **8. Email Encryption API Integration**

Digitally transforming business processes and workflow applications that handle sensitive information sometimes requires the encryption to be "baked in" or integrated with the application. Availability of a wide range of [email encryption APIs](#) from the provider, will give more control over how the API works with an app and should include:

- Messaging APIs. These are the APIs that send and retrieve data. Look for APIs that can handle multiple types of data, including email, files and form data.
- Administrative APIs. Password reset, managing users and their account settings, and integrating with Single Sign-On (SSO) are all features to look for.
- Provisioning APIs. Your API needs to grow with your application. Look for programmatic provisioning, servicing and on-boarding new users.

Full support from the API provider is another requirement. In addition to standard consulting and ongoing technical guidance be sure the vendor can provide:

- Multiple language support, including C#, VB.Net, Java and PHP, along with SOAP and REST.
- Technical reference guides that accurately document each API function and data structure. Sloppy documentation could indicate subpar operations.
- Demos for each programming language supported, including working sample applications with documented source code that demonstrates the implementation.

Lastly, be sure they can provide a pre-production sandbox environment. A full-service, fully-contained, pre-production environment allows you to quickly and safely create, test and preview your application.

# WHY IT PAYS TO PROTECT

## Data in motion

---

*There are risks and costs to a program of action — but they are far less than the long range cost of comfortable inaction. — John F. Kennedy*

---

### Government / Industry Regulation Requirements

Think HIPAA/HITECH, GLBA, PCI, FERPA, [State Information Security Laws](#), industry association data security best practices like [ALTA](#) (American Land Title Association), [NAR](#) (National Association of Realtors) and the [ABA](#) (American Bar Association). Non-compliance means your organization could end up paying large fines. In February of 2018, Fresenius Medical Care North America was faced with \$3.5 million in fines for five breaches, one of which was due to failing “to implement a mechanism to encrypt and decrypt ePHI, when it was reasonable and appropriate to do so under the circumstances.” Since 2015 over \$55 million in fines have been handed out to covered entities and their business associates that failed to comply with HIPAA regulations— and that’s just one set of regulations.

### Cost of a Data Breach

Although there is some expense involved in securing sensitive data in motion - there can be much higher costs for not securing it. Major data breaches are increasing in number, embarrassing and expensive. The [2018 study from Ponemon Institute](#) showed that in the U.S. the average cost of a data breach was \$233 per capita . This includes all sorts of variables that can easily escalate in cost – the costs of identifying the breach and applying all the legally required notifications, damage control such as support, investigation, remediation, fines and legal costs all add up. And that does not include the potential loss of business due to loss of reputation and customer churn.

The study shows the average cost per breach worldwide increased year over year, and the more records that are breached the higher the total cost. It gives the average cost for a breach of 10,000 records or less – at \$2.2 million. For over 50,000 records the cost climbs to nearly \$7 million, with mega breaches in the hundreds of millions. The study also says the chances of a company experiencing a data breach of 10,000 records is nearly 28% - that’s over one in four. The good news is the cost can be decreased by \$13 per capita through the use of encryption – which renders the data unusable and by another \$14 per capita by preparing ahead of time with an incident response team.



## State Department of Law Enforcement

*This case study discusses how a state agency responsible for fulfilling criminal background check requests transformed its workflow. It integrated secure data delivery with legacy systems, and eliminated major courier, fax and postal expenses for each background check delivered, while increasing document security, tracking and retrieval. Besides creating a more efficient faster workflow, costs were also greatly reduced, and the fulfillment operation, which was once operating at a loss, is now a major profit center.*

## Increase Profits by Transforming Workflows

Today's organizations need security solutions that are seamlessly integrated with applications and cloud services. This unlocks value as difficult compliance roadblocks that hold back business process improvements are paved into secure digital workflows. The availability of best-of-breed security solutions with comprehensive web services APIs, protocols and connectors now allows for easy, quick integration with an enterprise's other application suites – and from mobile apps to legacy mainframe if necessary. That's a powerful way to unlock more value for an enterprise while elevating the compliance profile – a big win-win.

## Published by **DataMotion**

DataMotion, Inc. provides PaaS (API) and SaaS (pre-built) solutions that redefine how organizations collaborate and share information with their customers and partners. Leaders in government, financial services, healthcare, insurance, and call center markets leverage our services to accelerate their business processes through modern, secure digital exchange. Our PaaS connectors and APIs enable secure, modern information exchange, allowing developers, software vendors and system integrators to enhance their solutions rapidly and seamlessly. In the healthcare sector, DataMotion is an accredited HISP (health information service provider), Certificate Authority (CA) and Registration Authority (RA) of Direct Secure Messaging. DataMotion is privately held and based in Morristown, N.J.



DataMotion, Inc.  
67 Park Place East, Suite 301  
Morristown, New Jersey 07960  
[datamotion.com](http://datamotion.com)

