Email Encryption for Government Organizations

8 Must-Know Insights for Email Security and Compliance
Email Encryption for Government Organizations

8 Must-Know Insights for Email Security and Compliance

In this guide:

I. The Decrypted Message Heard Round the World

II. Why Do Governments Need Email Encryption?

III. Email Encryption: 8 Must-Know Insights

IV. Introducing Virtru Client-Side Encryption for U.S. Governments
I. The Decrypted Message Heard Round the World

Poor encryption can ignite world wars. Just ask Arthur Zimmermann, the Foreign Secretary to the German Empire whose 1917 telegram to Mexico was decrypted by British codebreakers during World War I.

Zimmermann’s note revealed that, if the United States were to enter the war, Germany would seek a military alliance with the Mexican Government. He encrypted it using a German code and sent the message across telegraph cables that he believed to be safe – think 1917’s equivalent of email.

Little did Zimmerman know that the British government was watching.

The Brits cracked the code in just two weeks and gave the U.S. government the deciphered text. The ensuing backlash against Germany and Mexico helped draw America into WWI.

^ The Zimmermann telegram, as forwarded from Washington to Mexico.
II. Why Do Governments Need Email Encryption?

You might not realize it, but we send telegrams every day – over 34 billion of them.

Email is the modern telegraph, and the same problems that plagued Zimmerman – unsafe connections, weak encryption, reliance on third party communication providers – continues to expose governments to serious risks and repercussions.

In 2015, Chinese hackers accessed Office of Personnel Management (OPM) databases to steal the personal info of over 21 million federal employees and their family members. The stolen info included Social Security Numbers, birthdates, and even criminal background check data, which could be used by foreign enemies to blackmail U.S. government staffers into turning over classified info.

Could encryption have prevented the hack? Yes.

A 2014 inspector general’s report criticized the OPM for its “lack of encryption,” which other leaders highlighted as an “absolutely indefensible and outrageous” cause of the 2015 attacks.

Did government leaders adopt universal encryption following the OPM hacks? No.

Just months after the breach, teenagers hacked into CIA Director John Brennan’s personal email account, stealing Senate letters, phone logs, and other classified government documents – none of which were encrypted. In July 2016, Democratic National Convention chairwoman, Debbie Wasserman Schultz, resigned from her post after sensitive emails from her organization were leaked to reveal damaging intel about Hillary Clinton’s presidential bid.

As Brennan and Wasserman Schultz discovered, it is more difficult than ever for government organizations to secure the emails that they’re entrusted to protect – especially if those emails are not properly encrypted.
III. Email Encryption: 8 Must-Know Insights
When it comes to encryption, the problem is not awareness. With new email hacks each week, governments know that their online data is vulnerable, but it can be difficult to determine when and how to protect this sensitive info.

Which email compliance regulations apply to whom? What kind of encryption do cloud email providers enable by default, and is that enough? How can you ensure that your employees will use the security tools you give them?

Check out these eight must-know email security and compliance insights to find out:

1) Not All Email Encryption is Created Equal

Fort Knox, car doors, and bathroom stalls all use locks to keep out intruders. Does that mean one method is as safe as the other?

Of course not.

The same can be said for email encryption, which typically employs one of three methods for protection: point-to-point, portal-based, or client-side.

Point-to-Point Encryption (i.e., TLS)

Point-to-point encryption, such as transport level security (TLS), provides an encrypted pipe through which emails can be transmitted.

TLS ensures that unencrypted content is secure when traveling between mail servers, but it does not encrypt emails at rest. As a result, mail providers typically have access to the unencrypted messages that reach them throughout this process.
In order for TLS to work, both the sender’s and recipient’s email system must have TLS enabled. If the recipient’s server does not support TLS, the communication will not be allowed. This means the email will not reach its intended recipient.

Given these circumstances, and the fact that some email platforms do not support TLS, point-to-point encryption alone does not meet most government security requirements.

**Portal-Based Encryption**

Portal-based encryption tools add additional security for organizations by requiring new usernames and passwords to access sensitive content. Unencrypted plaintext is sent over a secure connection, but intermediate providers receive access to this unprotected content in the process.

This distinction means that portal-based providers manage the encryption keys and can see unencrypted versions of emails and attachments sent through their systems. This architecture introduces additional security risks and does not meet the requirements of certain regulations like ITAR and CJIS, which mandate that no intermediate party can ever have access to unencrypted content.
Only client-side encryption approaches ensure that content remains encrypted until it arrives on the intended recipient’s device. As a result, only senders and receivers ever have access to the decrypted email content, while third parties do not.

**Client-Side Encryption**

The problem with many encryption solutions, such as some TLS-based portals, is that, while they do encrypt your data, they cannot guarantee that your data is being transmitted between servers securely. Although the data might be secure when it leaves your computer, there’s no guarantee that it will remain that way on its journey to the intended recipient’s computer.
When you send a message over the Internet, that data is not just going directly to the recipient. Your message travels through — and in some cases, stays on — many different servers. Although you might believe all of those servers are secure, there’s a good chance that they are not. Even worse, it is entirely possible that one of those servers is monitoring every message it comes across.

Client-side encryption solves this problem by ensuring your message remains encrypted from the time you send it to the time it is received. Any servers it touches on the way to its destination will not be able to read it, as they will have no way to decrypt it — only the intended recipients will be able to use their keys to decrypt your message.

By preventing third parties from accessing your unencrypted content, client-side encryption enables government organizations to migrate to the cloud without sacrificing security or compliance.

2) Governments Require HIPAA Compliance, which Requires Email Encryption

The scariest compliance regulations are the most far-reaching ones. Created in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a compelling example of this.

HIPAA was enacted by the U.S. Congress to establish regulations regarding a variety of issues, including health insurance coverage, electronic billing, and the general transmission of protected health information (PHI). However, it applies to more than just healthcare organizations. If any of your employees ever deal with health-related data (i.e., citizen names, Social Security numbers (SSNs), medical record numbers, Driver’s License numbers, or even birthdates), you must comply with HIPAA policy, too.
Yes, this means most government organizations. Outside of healthcare, government employees exchange PHI more than any other industry, whether it’s via Health and Human Services Departments, welfare programs, Medicaid offices, public universities, or other groups.

In its Final Rule on HIPAA Security Standards, the U.S. Department of Health and Human Services (HHS) groups its required technical safeguards into four buckets:

a. Access controls
b. Audit controls
c. Integrity person or entity authentication
d. Transmission security

Of these areas, transmission security covers the bulk of email activities, and its requirements stem from one overarching HIPAA expectation:

“With respect to transmissions from covered entities, covered entities must protect electronic protected health information when they transmit that information” (pp. 8338).

This means that, as the HIPAA policy goes on to explain, organizations must “encrypt electronic protected health information whenever deemed appropriate” (pp. 8338).

In other words, if you share PHI via email, you must do so securely.

3) TLS Encryption Does Not Ensure HIPAA Compliance

TLS encryption ensures that communications sent to or from your mail server will remain encrypted when they travel through other servers that support TLS.

As a result, TLS-encrypted emails typically – but not always – meet the HIPAA standards for transmission security. If your email server supports TLS, you can compliantly share PHI in emails sent within your organization or to other organizations using TLS.

But what if you send emails to recipients who do not support TLS? Or what if your recipients share your messages with those who have unknown email environments?
Scenarios like these are particularly common for government employees. For example, you might be exchanging welfare applications with a constituent’s personal email address. Or maybe you’re sending medical records to a physician’s office.

In these examples, there is no way to ensure that your emails will remain HIPAA-compliant, no matter where they travel.

Client-side encryption, on the other hand, provides persistent HIPAA compliance by keeping PHI secure regardless of where it travels – and regardless of the recipient’s email environment.

4) Client-Side Encryption Can Enable CJIS Compliance in the Cloud

As valuable as client-side encryption is for HIPAA, it’s even more crucial for CJIS.

CJIS (Criminal Justice Information Services) is the largest division of the FBI. It monitors criminal activities in local and international communities using analytics and statistics provided by law enforcement. These databases provide a centralized source of criminal justice information (CJI) to agencies around the country.
The emergence of the Internet and cloud computing has changed data sharing drastically since CJIS was formed in 1992. To guard against the growing rate and sophistication of cybersecurity threats, CJIS developed a set of security standards for organizations, agencies, and technology vendors.

The policies set forth by CJIS cover best practices in wireless networking, remote access, data encryption, and authentication. The guidelines for email are rigorous, and rules related to “physically secure locations” confine most organizations to on-premise systems rather than the cloud.

However, the 2012 CJIS Cloud Computing Report provides a key option for CJI transmission in the cloud that reduces the compliance burdens of third-party email providers, while also preventing them from ever accessing an agency’s sensitive content. According to section G-26 of the report, “Encryption with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.”

When CJI is encrypted client-side, it is protected before it leaves a sender’s device or email client, and it remains encrypted until it reaches the intended recipient. Senders manage the encryption keys protecting their data. Therefore, if a user shared CJI via email with client-side encryption, that user’s email provider (or any third party, for that matter) would never have access to the content in unencrypted form since it would not have access to the keys needed to decrypt it.

This separation of keys and content enables governments to utilize cloud email providers, such as Google Apps and Microsoft Office 365, without sacrificing CJIS compliance or security.

As valuable as client-side encryption is for HIPAA, it’s even more crucial for CJIS.

**CJIS Hot Spots**

**Where to Look?**
- U.S. Federal Agencies
- Police Dept.
- Dept. of Corrections & Public Safety
- Attorney General’s Office
- Office of the Public Defender
- Office of the U.S. Courts
- Office of the County Sheriff
- Government Contractors

**What to Look For?**
- Arrest reports
- Fingerprint data
- Criminal background checks
- License plate numbers
- Protective orders
- Foreign identity information
- Sentencing and parole reports
- Body-worn camera footage
5) If You Use Encryption to Meet Compliance, You Also Need DLP

The toughest thing about compliance is that it frequently depends on people not screwing up.

That’s a tall order. The majority of data breaches are caused by user error.

Although many government organization have specialized security and compliance requirements, they all face the same fundamental problem: no matter how good the workplace training is, an employee can compromise HIPAA and CJIS compliance by emailing sensitive information to the wrong person, storing their login credentials on public devices, or even just setting a weak password.

Data Loss Prevention (DLP) tools eliminate these errors by scanning messages for PHI, CJI, and other sensitive info, and automatically encrypting any content that triggers certain preconfigured rules and policies.

For example, even if a police officer forgets to encrypt an email containing a victim’s license number, a DLP solution could scan that email, identify that number pattern as potentially sensitive, and automatically encrypt the email before it goes out.

Think of DLP as spell check for compliance.

Also, by notifying end users when and why they have triggered various rules, DLP can educate individuals about HIPAA and CJIS compliance, which helps foster long-term adoption of government policies and best practices.
6) When You Manage Your Encryption Keys, You Control Your Data

Have you ever sent an email you wish you could take back? Did you ever find out after the fact that someone forwarded a message that you wanted to keep private?

Email mishaps occur all the time. For government organizations, the stakes for these errors are particularly high. When you’re sending CJI and PHI, one misspelled recipient or premature click could result in 6-figure fines and months of bad publicity.

Luckily, certain types of encryption can minimize your exposure to these email blunders.

In order to prevent third parties from accessing unencrypted content, most client-side encryption software separates the storage locations of the content and the encryption keys used to protect it.

Emails are encrypted on the sender’s email client, and the encryption keys are stored on the encryption provider’s servers. Meanwhile, the encrypted email content gets sent out via the sender’s email provider, which stores this content for the sender and delivers it to the recipient. Once the encrypted content reaches the recipient’s email client, the encryption provider sends an encryption key to the client, enabling the recipient to view the decrypted email.

By separating the storage location of encryption keys and content, client-side encryption prevents your providers from getting access to your decrypted data. The encryption provider has access to the encryption keys, but not to your actual email content. The email provider has access to your email content, but it is encrypted, and
they do not have access to the encryption keys needed to decrypt the message.

This split-knowledge architecture provides enhanced control as well. Even though the encryption provider hosts the keys that protect your data, many solutions allow senders and admins to retain control over who can access these keys. When you control who can access these keys, you control who can read your encrypted emails – and when they can read them.

As a result, key management enables you to:

- Revoke any email, even after it’s been read
- Set expiration dates on emails
- Track where emails are forwarded, or disable forwarding altogether
- View read receipts to see when recipients have read your emails

While security is the top reason that most governments require encryption, these additional control capabilities can prove equally valuable when it comes to rectifying HIPAA and CJIS compliance mistakes.

7) When You Host Your Encryption Keys, You Choose Where Your Data is Stored

Would you give your team’s most valuable data to a potential enemy?

Neither would most federal governments. That’s why there are strict laws in place, such as CJIS, to ensure that government information is not stored in data centers outside of the United States.

But what if your email provider cannot guarantee that your data will remain in the United States after it leaves your premises? Or what if you have to share sensitive information with international recipients or colleagues who are travelling abroad?

That’s where customer-hosted keys come into play.

Customer-hosted keys enable you to store your encryption keys on your premises. Unlike most client-side encryption techniques, which store encryption keys on third-party servers, customer-hosted key management capabilities enable your organization to store encryption keys on your own cloud or in a physical Hardware Security Module (HSM).

As a result, customer-hosted keys make it possible for governments to:

- Enable easy-to-use client-side email encryption without having to trust third parties with encryption keys or unencrypted content.
- Ensure that you are the only entity that can respond to government access requests, such as subpoenas, since you maintain sole access to and ownership of encryption keys.
- Meet data residency requirements by specifying the locations where your encryption keys are stored.
- Destroy encryption keys to make emails permanently unreadable.

As more and more governments migrate to the cloud, customer-hosted encryption keys provide arguably the best way to safeguard your security process.
Not only do you manage access to the encryption keys, you host them. Your encrypted emails are unreadable without these keys, and since these keys are located wherever you choose, you decide where your unencrypted data can be accessed.

8) People Will Not Use Encryption if It Is Difficult-to-Use

This point may seem simple, but it’s a major reason that data breaches continue to plague seemingly obvious targets like the OPM and DNC. Email encryption is only as effective as it is easy-to-use.

Client-side encryption has existed for decades via a technique called public key encryption. Pretty Good Privacy (PGP) and S/MIME – two of the more common public key encryption technologies – were created in 1991 and 1995, respectively, but still have not been embraced by the government due to their technical complexities.

To start sending and receiving messages with either PGP or S/MIME, you need to install their software, generate a public and private key, register your public key, obtain your recipient’s public key, add it to your keyring, and encrypt your message — all before sending your message.

There’s no secure way to send a message to someone who hasn’t published a public key, and each message must be encrypted individually, meaning you can’t send group emails. And if you use PGP, but colleagues in another state or department use S/MIME, you have to install and learn both systems in order to exchange email with them. You also have to safeguard your own private key to prevent a thief from gaining access to all of your emails. You’ll also have to set up PGP or S/MIME and enter your key on every device you use, which wastes time and potentially exposes you to greater security risks.

Although PGP and S/MIME have the encryption basics needed for good security, they don’t have the convenience that modern government employees need.

When evaluating an email encryption solution, you must be aware of these user limitations before establishing your policy. While PGP and S/MIME set the standard for client-side encryption, new technologies have emerged to combine their security protections with a greater degree of ease of use.
IV. Introducing Virtru
Client-Side Encryption
for U.S. Governments
Compared with legacy approaches, Virtru provides the best of both security and ease of use. Public key-based technologies provide client-side encryption; however, they do so at the expense of usability.

Portal-based encryption technologies don’t encrypt the full path between the content’s sender and recipient. This unnecessarily exposes the content to eavesdroppers and can lead to a compliance violation or some other compromise of confidentiality.

With Virtru, you don’t just get better email security and HIPAA and CJIS compliance — you get total control over your secure email, a seamless Google or Microsoft experience, and convenience for users as well as for admins. In addition to client-side encryption, Virtru allows company admins to control forwarding, set expiration, and recall emails, so your organization’s data is protected at every step of the email’s journey.

Virtru integrates encryption into the email platforms that governments use, such as Gmail and Outlook, and allows end-users to set controls on their messages directly from the inbox.
Unlike TLS or portal solutions, Virtru doesn’t just encrypt your data in transit. Your message is encrypted from the moment you begin a new draft in Gmail or Outlook, so Virtru never has access to your email content. Because Virtru uses true client-side encryption, there are fewer points of vulnerability along your email’s path to your recipient’s inbox. Your message stays safe from beginning to end, and no third parties or cloud providers can access your data, including Virtru. Your agency or department maintains full control over your keys and your content.

Also, with Virtru, you can monitor data going in and out of your domain from a centralized dashboard. This feature just takes a minute to add to your domain, and your users only have to download a simple plug-in. You can track emails and attachments sent to or from anyone in your organization, while you control forwarding and revoke messages at any time. You can also trace where outgoing emails have been forwarded.
The best part? Virtru is convenient for both senders and recipients. You never have to leave your inbox to send and receive encrypted email. There are no extra credentials to remember. You don’t have to manually exchange keys with your recipient. To send an encrypted email, you simply click a switch, compose, and send your email as you normally would.

Administrators can ensure compliance with Virtru by easily configuring DLP rules to detect and automatically encrypt CJI before it ever leaves end-users’ devices.
Virtru also lets governments exclusively host and manage access to their encryption keys while still sending CJIS-compliant email. By allowing you to host these keys, Virtru’s Customer Key Server (CKS) helps you meet CJIS and data residency requirements in the cloud by specifying where unencrypted data can be accessed. No third party ever has access to these keys, and the CKS has no visible impact on the Virtru user interface.

By separating storage of encryption keys and encrypted content, Virtru prevents third party access to sensitive data, ensuring that governments have complete and exclusive access to their email content.
Given the rate at which cloud technology continues to evolve, it is important to stay up-to-date with how these developments impact government regulations.

As a thought leader in government compliance and encryption, Virtru offers a valuable array of resources to help you keep pace with the ever-changing digital landscape:

**Blog Post:** [CJIS Compliance and Data Encryption – Here’s What You Need to Know](#)

**Blog Post:** [HIPAA Compliant Email Encryption: Looking Beyond Portals](#)

**Webinar:** [Secure Your Org: A Practical Guide and Case Study on Email Encryption](#)

**Case Study:** [How Virtru Shows Columbia County Employees When to Encrypt](#)

**Case Study:** [Virtru Brings Email Security and Compliance to Pitkin County](#)
Email Encryption Needs Assessment Checklist for Government

While there are several components to CJIS and HIPAA compliance that are unrelated to email, these exchanges pose some of the biggest risks for government data leaks. As a result, it’s critical that you take inventory of your team’s best and worst data security practices.

The following checklist will help you to evaluate your organization’s need for email encryption and determine appropriate solutions to meet your related compliance requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes or No?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do any employees at your organization have access to CJI or PHI?</td>
<td></td>
</tr>
<tr>
<td>If yes, do these employees ever share CJI or PHI via email?</td>
<td></td>
</tr>
<tr>
<td>Does a cloud provider like Google or Microsoft host email services for those employees who have access to CJI or PHI?</td>
<td></td>
</tr>
<tr>
<td>If yes, do you have CJIS SLAs and HIPAA BAAs with these vendors?</td>
<td></td>
</tr>
<tr>
<td>Does your cloud provider meet the standards of FIPS 140-2?</td>
<td></td>
</tr>
<tr>
<td>Have you conducted criminal background checks for all employees responsible for managing the cloud services your organization uses?</td>
<td></td>
</tr>
<tr>
<td>Does your cloud provider guarantee that your organization’s email data will not leave U.S.-based servers?</td>
<td></td>
</tr>
<tr>
<td>Does your organization use any type of email encryption?</td>
<td></td>
</tr>
<tr>
<td>Is the encryption your organization uses at least 128 bit?</td>
<td></td>
</tr>
<tr>
<td>Does your encryption protect emails both at rest and in-transit?</td>
<td></td>
</tr>
<tr>
<td>Do personnel use client-side encryption to share sensitive data?</td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Yes or No?</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Do you utilize DLP to prevent unintended users from gaining access to sensitive CJI and PHI?</td>
<td></td>
</tr>
<tr>
<td>Would you prefer to use a centralized platform for all of your organization's confidential and non-confidential communications?</td>
<td></td>
</tr>
<tr>
<td>Are you required to store certain sensitive email data within the U.S.?</td>
<td></td>
</tr>
</tbody>
</table>

**Enhance Your Email Security Today**

Whether you are already using a cloud service like Google or Microsoft, or are looking for stronger on-premise security, [Virtru’s government email encryption](https://www.virtru.com) is the easiest, most secure way to comply with privacy and compliance standards. To see if Virtru is right for your organization, you can:

- [Download Virtru for free now](https://www.virtru.com) and start sending securely
- Contact us to [request a demo](https://www.virtru.com)

**About Virtru**

By combining military grade encryption, cloud-based access and controls, and seamless integration with applications like Google Apps for Work and Microsoft Exchange, Virtru enables security without getting in your way. Whether for regulatory compliance, data security, or corporate privacy, Virtru is the easiest way to protect sensitive information.

[www.virtru.com](https://www.virtru.com)
[sales@virtru.com](mailto:sales@virtru.com)