Secure Healthcare Payer Communications: Best Practices & Compliance Tips

clarity®

organize customize deliver®

Healthcare payer organizations are at the heart of a robust and dynamic health ecosystem.

By enabling efficient information flow between various health service providers, healthcare payer organizations play a pivotal role in facilitating effective patient care. However, the sensitive nature of health data makes secure communication critical within these organizations.

There's no denying the healthcare industry faces several challenges in this space due to the sensitive nature of patient information, including:

- Ensuring all Protected Health Information (PHI) is safeguarded
- Complying with the Health Insurance Portability and Accountability Act (HIPAA)
- Preparing for possible data breaches and other cyber attacks
- Coordinating seamless communication between multiple healthcare entities
- Evolving standards to fit the telehealth model

One way to address these challenges is to stay up to date on best practices and compliance tips for healthcare communications.

Below, we'll address the key pillars for understanding these practices, how they impact healthcare communications, and what healthcare organizations can do to secure PHI while still creating a comprehensive and engaging communications plan.

Putting the Best in Best Practice

Understanding the Regulatory Landscape

Anyone overseeing and interacting with healthcare communications must understand the associated regulations and compliance standards.

These are in place to protect PHI and provide healthcare organizations with guidelines on how to do so.

Some of these regulations and standards include:

1. **The Health Insurance Portability and Accountability Act (HIPAA):** This federal law requires healthcare organizations to adhere to standards protecting PHI and ensure that information isn't shared without a patient's knowledge and consent.
2. **Health Level Seven (HL7):** This is an internationally-recognized set of standards for the exchange, integration, sharing, and retrieval of electronic health information. It provides a framework for seamless interoperability and communication between different healthcare organizations and applications.
3. **International Classification of Diseases (ICD):** This international diagnostic tool is used to catalog what causes injury and death and provides the standard for how to do so.

Not complying with regulations and standards established to protect sensitive data and PHI can lead to serious consequences. For instance, noncompliance with HIPAA can result in:

- Fines ranging from $100 to $50,000 per violation, depending on the severity of negligence
- Lawsuits being brought against perpetrators

Best Practices for Secure Healthcare Communications

Any organization handling PHI needs to follow best practices for secure healthcare communications to mitigate risk and ensure sensitive patient information is protected. These best practices include:

1. Implementing secure communication channels

Securing your communication channels reduces the risk of PHI being compromised.

Tips for securing these channels include:

- **Encrypting email systems:** Encrypting email systems helps prevent unauthorized individuals from accessing sensitive messages and compromising information.
- **Securing messaging platforms where PHI is transmitted:** Securing these messaging platforms reduces the risk of data breaches.
- **Installing virtual private networks (VPNs) to encrypt internet use and access:** Installing a VPN protects sensitive data and helps healthcare workers remain private online while crafting communications.

2. Ensuring authentication and access control

Another way to secure healthcare communications is to ensure there's an authentication process and tight access control in place.

Authentication allows systems to verify who specifically is accessing and handling data. Having strict access control policies limits the number of people who can obtain sensitive information and, as such, reduces the risk of that information being compromised.

Strategies for ensuring authentication and access control include:

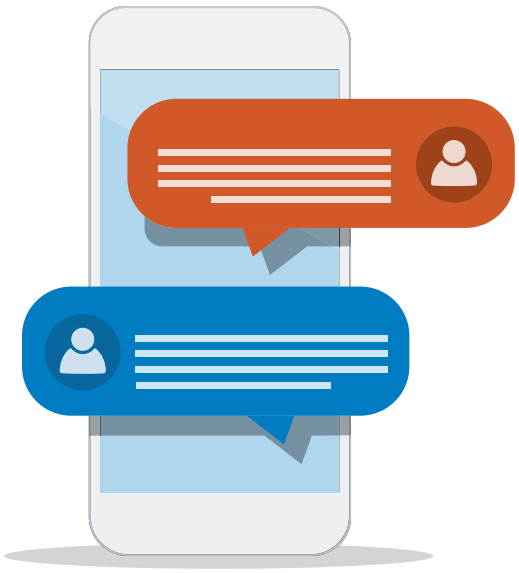
- **Implementing strong password policies**
- **Setting up two-factor authentication**
- **Establishing role-based access controls**
- **Educating employees on security protocols**

Best Practices for Secure Healthcare Communications

3. Regularly updating and patching systems

Maintaining and updating your systems is an essential step in securing your healthcare communications. If your systems are outdated, your security is likely not as strong as it should be, leaving sensitive information at risk.

On a similar note, patching your systems is crucial for securing communications. Patches will resolve software issues that leave systems vulnerable, while simultaneously improving functionality.



Key ways to maintain systems include:

- **Creating training programs on secure communication practices for staff**
- **Regularly scheduling awareness campaigns and updates**
- **Informing staff of the importance of software and system updates**
- **Enacting patch management strategies across systems**

Privacy and Confidentiality Considerations

We can't talk about secure healthcare communications without mentioning the importance of data privacy and confidentiality. Prioritizing the protection of sensitive data is a non-negotiable in any organization or facility handling PHI.

How to prioritize patient data protection

There are several ways to prioritize data protection within your organization. These include:

1. Complying with HIPAA

As previously stated, adhering to HIPAA is essential for healthcare organizations handling PHI, which includes laboratory test results, billing details, and other information that can be used to identify a patient.

Not complying with HIPAA can lead to severe legal and financial consequences, including fines, jail time, and possible lawsuits.

Plus, an organization's reputation could be negatively affected if it has a HIPAA violation on its record.

2. Encrypting and anonymizing patient information

Encrypting and anonymizing patient information adds additional layers of security to PHI, protecting this sensitive information and reducing the risk of it being compromised.

3. Minimizing data breaches and unauthorized access

This can be done with the secure storage and safe transmission of data, monitoring and auditing access logs, and implementing secure file-sharing platforms.

There are no ifs, ands, or buts about it.

Organizations sending healthcare communications need to protect patient data while engaging members with their correspondence. Not only is it a legal and ethical responsibility, but it is also crucial for building trust and maintaining the reputation of the organization.

By safeguarding patient data, organizations can effectively engage members through their correspondence, providing personalized and secure communications that prioritize privacy and confidentiality.

The Clarity team understands this critical pillar of communication and offers an enterprise solution that prioritizes privacy and confidentiality while creating engaging healthcare communications. We invite you to view **our solutions** and harness the tools for complete control over your communications.

Compliance Tips for Secure Healthcare Communications

By taking the right precautions and implementing the right strategies, healthcare organizations can establish a reliable compliance plan for their communications.

The following tips can assist healthcare teams ensure compliance while crafting and sending correspondence:

1. **Conduct regular risk assessments and audits:** Regularly assessing risk helps identify any gaps in compliance, allowing organizations to make swift changes that mitigate those concerns.
2. **Establish incident response plans:** If an incident does occur, having an established incident response plan provides a clear guide on what to do and how to do it, reducing confusion and increasing overall response efficiency.
3. **Engage third-party vendors with robust security measures:** If you work with third-party vendors, make sure they too have robust security measures to protect PHI and strengthen the confidence of your partnerships.
4. **Stay updated on industry trends and emerging threats:** You don't know what you don't know. Keeping up with industry trends and emerging threats makes you more knowledgeable and helps you prepare for any new situations that may arise.
5. **Collaborate with legal and compliance teams:** Working with your legal and compliance teams opens several avenues for education and collaboration, ensuring everyone is informed of risks, best practices, and new procedures.
6. **Address the human factor:** One of the most important compliance tips is to recognize and address the human factor, or the role of human error in security breaches.

   Organizations can put every plan in place and stress the importance of compliance, but at the end of the day, humans are…well, human, and humans make mistakes. That's why it's important to account for this factor and do what you can to minimize the risk of human error.

   This includes training employees on identifying and avoiding common security pitfalls and encouraging a culture of security awareness and reporting.

The Importance of Secure Healthcare Communications

If there's one thing you take away from these best practices and compliance tips, let it be this:

It's essential for any person or organization creating and sending healthcare communications to protect PHI.

Not having secure and compliant healthcare communications can get you in legal and financial trouble. Plus, your brand reputation could be at stake if there's a serious violation.

You can have secure healthcare communications by being aware of your ethical and legal obligations, having plans in place to ensure compliance, and training your staff on the importance of security and compliance with PHI.

It's also crucial to stay on top of emerging trends and threats, striving for continuous improvement.

Organizations must also have the willingness and ability to adapt as security threats change and evolve.

As technology advances and nefarious entities find more sophisticated ways to access sensitive data, healthcare organizations must remain vigilant about protecting PHI without sacrificing the quality of their communications.

Given the pressures of the modern healthcare organizational landscape, it can be hard for leaders to ensure these communications are secure and still contribute to their overall communication goals.

One solution is to work with an outside vendor, like Clarity.

Our platform harnesses the power of data to create engaging healthcare communications, from member guides and letters to ID cards, EOBs, and more.

Request a demo of our platform today and learn how to increase member engagement effectively and securely.