LUXSCI®

How to Minimize the Risk of Breaches with HIPAA-Compliant Email

Accidentally causing a data breach is as easy as clicking ‘Send’. Follow LuxSci’s tips for HIPAA-compliant email & minimize your business’ risks.

Data breaches are emerging as one of a company’s greatest fears. When you consider the recovery costs, reparations, penalties, and the ensuing investment in new security measures, data breaches can wind up being incredibly expensive. And that’s without accounting for the disruption to normal business, or the long-term damage to a brand’s reputation.

Sony estimated its 2011 hack would end up costing it $171 million, so data breaches are hardly a threat that can be shrugged off. Companies in the health field face even more complex threats, because they have to worry about HIPAA regulations and protecting the personal data of their patients.

One of the key risks is email. Not only is it a major attack vector, but improper email use can easily lead to electronic protected health information (ePHI) being accidentally exposed. Email is such a banal and everyday form of communication, that many people rarely consider the potential ramifications of what they send. This makes it trivial for an employee to mistakenly leak someone’s personal data without even thinking about it.

A benefit of the HIPAA regulations is that they aren’t some arbitrary set of hoops that the government forces businesses to jump through. If organizations follow the recommendations, HIPAA actually sets up a solid foundation of security practices and policies that help to protect everything from emails to entire organizations.

HIPAA sets up a solid foundation of security practices and policy.

The Approach Is as Important as the Specifics

The HIPAA regulations aren't a checklist of every specific measure or technology that organizations need in order to secure their data. This kind of approach would be inflexible, causing unnecessary burdens on small businesses and not matching the needs of enterprises. Due to the slow pace of legislation, specific regulations wouldn't be able to keep up with the rapid advance of technology, resulting in an insecure and unusable system.

Instead, the regulations are open. They list an overall approach as well as where control measures need to be in place, then deem them as either 'addressable' or 'required'. Some seemingly essential security aspects like encryption are only deemed addressable. But if you try to use this as a loophole to avoid encryption, your organization is going to end up in trouble.

The regulations are written this way to give organizations the freedom to choose the most appropriate security measures for their unique situations. While a company doesn't technically have to implement encryption, it does have to undergo a thorough security analysis and adopt the appropriate measures to protect its ePHI.

Guess what? Any reasonable analysis will tell you that encryption is the most appropriate way to make data confidential both in transit and at rest.

How Does HIPAA Apply to Email Security?

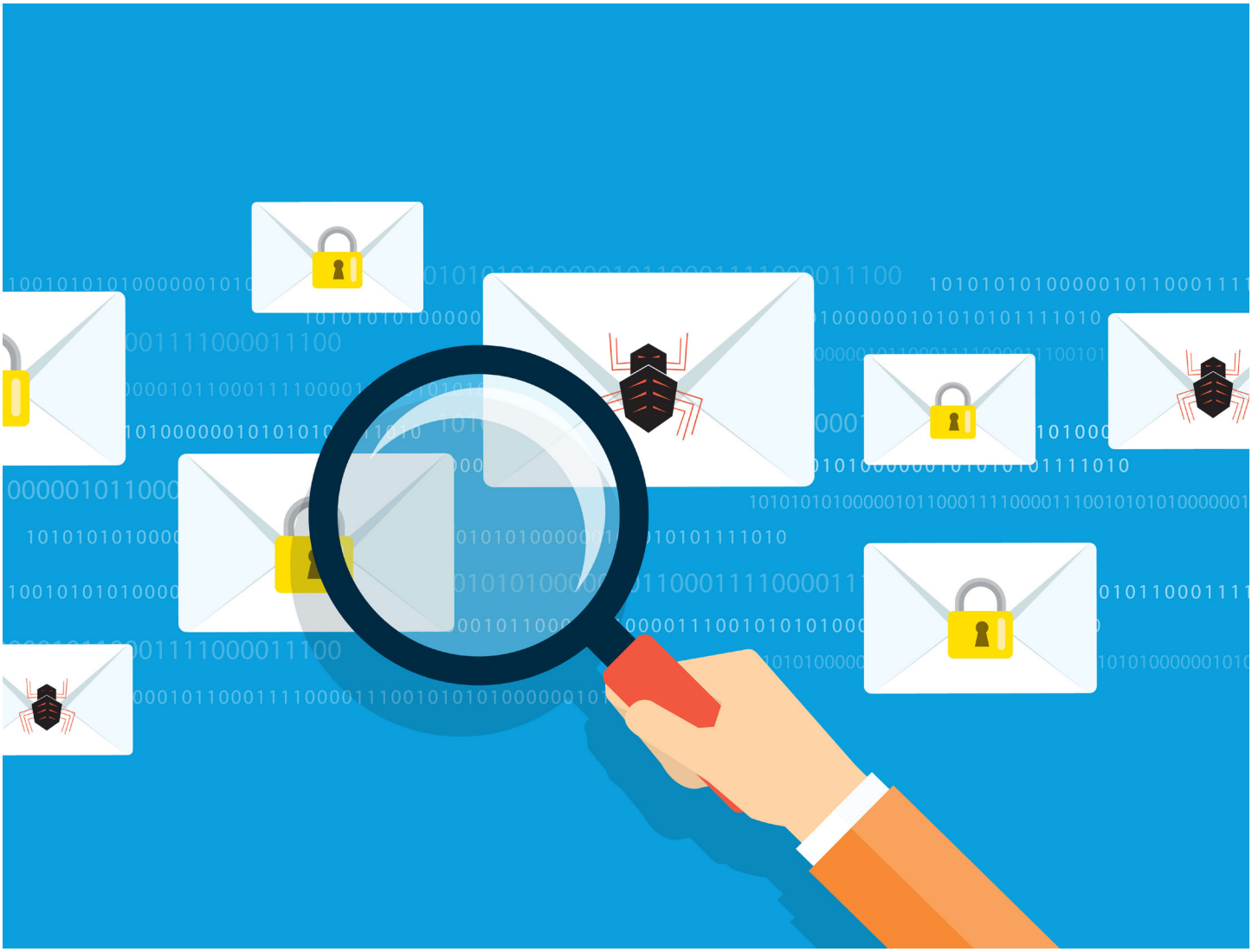
As part of your organization's overall security and HIPAA-compliance strategies, it will need to regularly evaluate the practices, procedures and policies that surround its use of email. In this review, it needs to pinpoint the key risks, especially when it comes to ePHI. Your company then has to use HIPAA's recommendations as a basis to implement appropriate mitigation strategies.

Three aspects of HIPAA are particularly important when it comes to email:

- **Authentication mechanisms are required** – Procedures need to be in place to verify that only authorized individuals are granted access and that everyone has a unique authorization.

- **Transmission security is addressable** – These are controls that safeguard the integrity and confidentiality of the data.

- **Business associate agreements (BAA) are required** if a third party is involved in processing your organization's ePHI.



When companies complete their email security analyses, they will all come to the conclusion that they need access control, encryption, measures to ensure data integrity, and much more. Some will find that they need more advanced mechanisms than others, such as opt-out email encryption to reduce the chances of employees accidentally causing data breaches.

Ultimately, some businesses may decide that they have the capabilities to make their emails HIPAA-compliant in-house. Others will choose to go with a HIPAA-compliant provider that specializes in dealing with the complex regulatory world. This approach is generally easier, and helps to spread the risks onto the provider, as long as a BAA is signed.

The end result of either approach will be more than just HIPAA compliance. If your company has been judiciously following HIPAA's recommended path of performing security reviews and implementing mitigation strategies, then it will end up with a secure email system as well. With the right systems in place, your organization will reduce its chances of suffering a data breach.

LUXSCI®

Have Additional Questions? We're Happy to Help!

Call: **+1 800-441-6612**

Email: **sales@luxsci.com**

Web: **luxsci.com**

Solutions to Ensure Your Private Information Stays Private:

- Secure Email
- Secure Websites
- Secure Web & PDF Forms
- Secure Text
- Secure Chat
- Secure Email Marketing
- Secure Video

LuxSci is your trusted leader for secure email, data and communication solutions. LuxSci helps ensure that "what's private stays private." Find out why LuxSci is the go-to source by the nation's most influential institutions in healthcare, finance and government for comprehensive, flexible, and easy-to-use secure solutions.