



# New HIPAA Rules Putting the Spotlight on Email Encryption

As electronic communications becomes more pervasive in the healthcare industry, the rules governing the protection of information, including email transmissions, have come under increasing legislative scrutiny. With recent changes to HIPAA legislation in particular, the healthcare industry and partners are having to rethink their communication practices, including encryption.

It stands to reason that any entity sending patient health information (PHI) over the Internet needs to encrypt it. Using standard email is tantamount to writing a letter and not putting it in an envelope so anyone can read it. In the HIPAA world, any element within an email (e.g. sending a lab report to a physician) that provides a context, such as the patient's name, social security number or anything else that would identify them, must be protected.

In their efforts to minimize risk and avoid the fallout from human error, many entities that fall under HIPAA guidelines have resorted to faxing or using couriers to deliver sensitive information. "The industry is being extremely cautious as a general rule," notes Abner Weintraub, President and Chief Executive Officer of HIPAA Group Inc. "The general response to HIPAA and email has been a 'don't do it' approach. So the healthcare community is still heavily reliant on couriers, online storage and drop boxes. That's partly due to the confusion in terms of what the law prohibits, allows or restricts."

All that is changing however as we witness an ever growing need to leverage email as a means of communication. As a result, encryption technologies to facilitate secure email delivery are becoming an integral part of the HIPAA conversation.

## The New Face of HIPAA

Recent changes to HIPAA contained within Section 164 of the HITECH Act (part of the Recovery and Reinvestment Act), which came into effect in February, 2010, have applied much more stringent enforcement and penalties, as well as increased disclosure requirements for even the most minor of breaches.

Another extremely significant change has been the extension of HIPAA compliance to business associates of hospitals, which can include testing laboratories, pharmaceutical firms, and any other organizations communicating with physicians and/or healthcare facilities. This has at least tripled the number of entities that must comply with HIPAA standards.

A key component of Section 164 of HIPAA is transmission standards which require that all IT staff of any healthcare firm or covered entity need to:

- A secure, "strong" encryption services platform that uses industry standard PKI (public key infrastructure) and S/MIME technologies.
- Select a method of protection and comment on why they implemented it.

In simple terms, that means identifying what information you are sending out, how it is protected, what you chose, and why. Given the scope of this mandate, it is evident that email encryption will play an increasingly critical role in helping organizations meet these new legislative mandates.

*[continued on next page]*

*[continued from previous page]*

Even when taking standard precautionary measures (e.g. staff training, courier delivery, etc.), email-based HIPAA violations occur often. These for the most part tend to be accidental, such as sending an unencrypted note that contains patient health information to an incorrect address. Under the new legislation however, the ramifications of these types of oversight are extreme. Each incident of that nature represents a data breach that must be reported by law within a certain time frame to major media.

“The issue of breach notification has shaken up the industry,” Weintraub explains. “But something that has been overlooked in the furor but is critically important, is that if emails are shown to be properly encrypted and secured and a breach of data occurs, no disclosure to patients, consumers or the Health and Human Services needs to be reported.”

## Encryption Now

That apprehension is being overcome as encryption technologies improve in terms of efficiency, ease of use and interoperability. Policy-based encrypted gateway services for example offer a viable and affordable alternative that allows entities to enforce email encryption behind the scenes without disrupting the day to day workflow of employees.

With this type of managed DLP (data loss prevention) encryption solution, administrators can define policies around company confidential data that is being shared over the Internet.

The service works as follows:

- All correspondence is scanned on the premises or in the cloud based on established policies.
- Built-in dictionaries or lexicons search through each email (including attachments) to identify elements at risk, such as social security numbers, drug codes, patient names, etc. and then automatically encrypt them when required.
- Any emails using that domain – whether via a smartphone, laptop or desktop system – are automatically scanned using the same policies

The value of this level of efficiency is enormous. It not only relieves the burden of extensive training efforts, it also reduces the costs and complexities of managing encryption in-house. IT managers can use a Web-based console to know what email is going out, the criticality and nature of the data and who is sending it; as well as set, review and customize privacy policies so confidential contents is automatically encrypted. This enables them to easily identify potential data breaches and apply the appropriate safeguards.

Automated encryption based on defined business rules will become an essential part of HIPAA compliance moving forward. A managed service model can speed deployment, ensure interoperability with existing systems and processes, and eliminate the risk of human error.

### About Echoworx

Echoworx Corporation is the leading provider of managed encryption services for complete enterprise email and data protection. The company is an encryption service provider of choice for Symantec, AT&T, Verizon, BT and Apptix among other global enterprises. Echoworx provides a SaaS (software as a service model); it is built on best-of-breed technology and reduces encryption complexity for the end user. With Echoworx, organizations can protect their email and data without changing their day to day workflow and can easily send encrypted documents and digitally signed email messages to anyone in their address book. For more information: [www.echoworx.com](http://www.echoworx.com)