



Are your E-mails Compliant with the Massachusetts Data Protection Law?

The Massachusetts data protection law, [MGL 93H & 201 CMR 17.00](#), requires that businesses comply with various data encryption requirements: “To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.”

What Does this Mean?

Simply stated, “encryption is a technical process that makes it nearly impossible for an unauthorized individual to access the contents of a file or message.”

Encryption is especially important with e-mail transmission between HR Knowledge and our clients.

Businesses use a variety of programs to write and send e-mail, such as Gmail or Outlook, as well as mobile devices such as a BlackBerry, Droid or iPhone. It makes communications from one business to another nearly instantaneous, but also increases the risk of exposure. For those of us in states that have data protection laws, it is potentially a violation if we don’t have the proper measures in place.

How Does E-mail Work?

Email is typically sent in this fashion:

- The sender’s email client (e.g. Outlook) sends an email through the sender’s email server.
- The sender’s server sends the email to the recipient’s server using the SMTP protocol.
- The recipient downloads the email from the recipient’s server.

Unfortunately, this process is not secure. SMTP by its nature sends the email unencrypted (meaning in a format that anyone can read). Since the message or attachments may contain sensitive information -- your employees’ benefit enrollment, home address, social security number, birth date and details about all their dependents -- that message could be read by anyone along the path from sender to recipient, whether by users who manage a hosted antispam service or even by your company’s network administrator. The unauthorized user could be running a filter that looks for "social security" "birth date" or credit card information.

What Should I Do to Protect My Employees’ Personal Information?

If you conduct business in Massachusetts, you are required to comply with the data security protection law and protect employee and customer personal information.

There are different ways to send encrypted e-mails. Each will require a different level of effort and cost to setup, implement or use, and each will require that both parties in a communication understand enough about encryption to use it.

HR Knowledge has ensured compliance with the Massachusetts data privacy law by protecting its communications using two different methods. We encrypt all messages that contain personal information using the trusted, Cisco Ironport solution. If your mail system (server) supports a particular type of



encryption, then you, as the recipient, do not need to do anything out of the ordinary. You will receive the mail in your Outlook or on your smartphone as you always do, but you can rest assured that the message will have been completely encrypted from the moment that we sent it until the moment that it arrived in your mailbox.

Additionally, we have setup a system called ShareFile which allows encrypted communications for those whose mail systems may not support the required encryption processes. Although this takes email out of the communications loop, it provides a very easy-to-use method of sending you the information which otherwise would have been sent as a message attachment. You will simply receive a message indicating that you have a file waiting, and you will then login to a website from which you can download the file. The download process is completely encrypted. Similarly, you can transfer sensitive files to us using this method, a process which is not possible using our Cisco Ironport solution.

If you have had difficulty receiving encrypted email attachments from us, or if you require a mechanism to send sensitive information to us, please contact your HR Knowledge account manager to arrange a no-cost account on this new system.

This content is provided with the understanding that HR Knowledge is not rendering legal advice. While every effort is made to provide current information, the law changes regularly and laws may vary depending on the state or municipality. The material is made available for informational purposes only and is not a substitute for legal advice or your professional judgment. You should review applicable laws in your jurisdiction and consult experienced counsel for legal advice. If you have any questions regarding this advisory, please contact HR Knowledge at 508.339.1300 or email us at HR@hrknowledge.com.