HIPAA Compliance Tricks & Treats

There's rarely a week that goes by where I don't get a call from one of our agent partners asking, "How do I protect myself from hackers and compliance violations?"

These are important questions that should be asked by everyone who handles Protected Health Information (PHI) and Personally Identifiable Information (PII) to ensure Health Insurance Portability and Accountability Act (HIPAA) compliance. Don't worry, you don't have to be a security expert to keep you and your client's personal data safe.

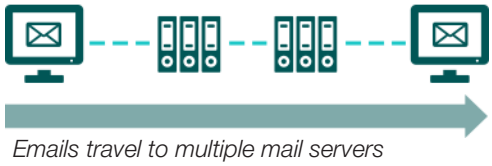
Discover the tricks used to steal your information and the treats of how to stop them.

Secure Your Emails

Trick: Your emails can be intercepted multiple times before being delivered.

Believe it or not, faxes are considered a method of secure communication, but regular email is not. That's because when you send an email your message bounces from one mail server to another before being delivered to the recipient's inbox, giving hackers multiple chances to steal your data before it's even delivered. Whereas when you send a fax the data is sent from one device to another without anything in between, also known as point-to-point.

Faxes are sent directly from one machine to another.



Emails travel to multiple mail servers before being delivered.

Treat: Encrypt your emails.

One way to send emails securely for compliance is by using an email encryption service. Services like this encrypt the email for you, and the email recipient receives a notification in their inbox directing them to login to a secure web site to see the protected content. You can search for "secure email providers" online to find a company that can assist you in protecting this sensitive information.

Secure Your Computer

Trick: If your hard drive is stolen it's easy to get your information.
One of the most common problems that leads to PHI and PII being leaked to the public, scammers, or thieves, is theft of laptop and desktop computers.

Treat: Encrypt your computer.
A simple solution that is included in Windows 10 Pro, Enterprise and Education versions is Bitlocker. Bitlocker is Microsoft's drive encryption suite that protects systems by putting a password on the hard drive. As soon as you press the power button on your computer and it starts up you will be immediately prompted for this special password or pin to allow the hard drive to be accessed. The Bitlocker process does not replace your current Windows login, it works in conjunction with it.

Once your valid password is entered, the Windows operating system will load, prompting you to login the way normally would. Anytime your system is restarted or gets turned on from a powerless state you would be prompted for your Bitlocker password. Encryption ensures that even if your hard drive is removed from your computer the information on that drive cannot be accessed, and all your content is safe.

Don't Be Afraid of Compliance

Trying to be compliant can be a scary task in this technological age where thieves and hackers are around every turn. My advice is to find a company who is competent in computer and data security so you can make the best effort to ensure you are securing protected health information and personally identifiable information.

Downloadable Resources

- Best Practices for Handling Personally Identifiable Information: Fast Facts for Assisters (DHS)
- Handbook for Safeguarding Sensitive Personally Identifiable Information (HHS)

Visit our website at www.urlinsgroup.com/aries or contact us at 1-800-926-8875 to see how you can start saving time and making money today!