



INTERNET E-MAIL SECURITY

According to the Identity Theft Resource Center, hackers exposed approximately 220 million personal records in 2009. Of this total, more than 11 million were categorized as 'Medical/Healthcare' records. Numbers like this are often achieved because an underlying account or data transfer is compromised, creating many record exposures from a single event.

One event started as a suspected breach of 10,000 Hotmail accounts and grew in just days to affect an estimated 30,000 email users. The list of providers affected also expanded beyond Hotmail to include accounts hosted by Gmail, Yahoo, AOL, Comcast and EarthLink. Hackers posted the usernames and passwords for breached email accounts on a public website where anyone was able to view them. Email providers warned, or in some cases forced, the owners of compromised accounts to change their password.

This attack was carried out through a phishing scam. Phishing is the practice of luring users to a fake website designed to look authentic in an attempt to steal passwords, financial or personal information, or introduce a virus. Phishing is a common avenue of attack for Hotmail, Yahoo and Gmail accounts. Hackers know that many people use these email services, since they are free and accounts are easy to acquire. But, security and convenience are often at odds.

To help protect email transmissions, Gateway Health Plan® has implemented a secure email solution. For those companies that have email systems that support end-to-end encryption, when a Gateway employee flags an email as 'secure', the work is all done behind the scenes. These emails are sent securely without the receiver needing to do anything different. They simply show up in a recipient's inbox like any other email.

If companies are using an incompatible email system, they will need to go through Gateway's secure portal to retrieve the email. Accessing the portal requires setting up an account and password. Once access is gained, users can receive and reply to Gateway emails in a secure manner. Forgotten passwords can be reset using information listed on the portal by simply following the steps as outlined.

If at all possible, emails to and from organizations should utilize internal corporate email servers instead of less secure or free email services. While some of these email providers offer encryption protection, it is not usually enabled by default. However, even when this option is selected, it only protects the email for part of the journey across the Internet.

HIPAA security standards are in place to specifically address protecting health information that is sent electronically as well as mechanisms to encrypt and decrypt this information. The American Recovery and Reinvestment Act of 2009 (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) contain several HIPAA regulations and the penalties are tougher than ever. Therefore, it's especially important to take additional precautions, such as using secure email, to reduce the likelihood of a breach.

Gateway has made the security of sensitive information a priority. Please take all reasonable precautions when transmitting provider, member, and health plan information via email.