



SECURITY AND HIPAA

Frequently we are asked about HIPAA and security as it relates to our web-based iNetiPass and iNetiCare solutions. Being a leader in providing online claims and care management services, iNetico has addressed internet security and electronic protected health information (PHI) security within the system design.

So what is PHI? HIPAA regulations define protected health information as “any information, whether oral or recorded in any form or medium” that “is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse” and “relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”

That covers a lot of information territory, so what does it not cover in regards to data interchange? It does not specifically cover in-person voice communications, telephone calls, and paper transmissions such as paper-to-paper faxes, voice messages, and video conferencing. It does cover all other mediums including EDI, telephone voice response, and “faxback” systems. Remember again that the Privacy Rule is normally interpreted as requiring appropriate security measures for PHI of all kinds so everything is covered to some degree.

When accessing iNetico web based programs, users can feel self-assured that the data they are viewing is secure with 128-bit encryption by locating the browser’s lock symbol on their screen. iNetico provides additional peace of mind with Thawte credentials displayed at the bottom right hand side of the screen. Thawte is a third party provider of identity verification software that creates an encryption layer between our servers and your web browser via an encryption key. This encryption ensures that data exchanged in the connection is not plainly viewable to others. This is the first layer of security within the iNetico online claims and care solutions.

The second layer of security is contained within our logon process. This is the layer that applies user level security accesses and individualized system access options upon logon. All users are assigned a unique login id and a password that expires every 90 days. Additions, terminations, and maintenance of login id’s and their profile information is manageable directly by you, our client or partner.

The third layer of security is provided by our session monitoring and timeout. Users that walk away from a live session in iNetipass or iNeticare can rely on iNetico to auto-terminate the session after 20 minutes of inactivity leaving sensitive PHI secure from wandering eyes.

Our last layers of security occur within our network securing all PHI on separate password protected data and web servers. iNetico also maintains our own hosted environment at our secure corporate location. We do not co-locate our servers with any other firms so we can ensure data security and integrity. Additionally, our network and programming engineers are certified yearly by our onsite HIPAA security compliance officer. This highly trained and specialized team ensures our network security, daily system backups, and maintains a solid disaster recovery plan.

The iNetipass and iNetiCare systems are proprietary in-house developed software solutions. We do not rely on third party software and we have full control over the security picture. For the complete security package to be effective, remember that it must be applied to the whole system including all administrative, physical, and technical safeguards.

I could discuss all of our security features in a large novel, yet I encourage you to experience the capabilities and design first hand. If you have not had the opportunity to walk through the iNetico solution, I encourage you to arrange a personalized webinar to learn more about its features and security.

By Cliff Palmer, iNetico CIO