- ClaimsLink Configuration Guidelines -

Last revised: 24 January 2012

Table of Contents

Overview

Medical Mutual developed ClaimsLink and other Internet services to provide its policyholders, providers, and other external customers with an easy, convenient way to obtain information related to eligibility and claim payments. However, we also recognize our obligation to protect the privacy of this information. Security has always been of paramount importance to everyone on the development team. This document will describe both the configuration requirements for using ClaimsLink, and the techniques being used to keep policyholder data confidential.

The fundamental requirement is to establish secure sessions with authorized site visitors. In other words, we must be able to send and receive data in a way that prevents unauthorized access to the information exchanged with authorized site visitors. These private communication sessions must not be penetrated by external parties, and sensitive information must be protected from unauthorized access. Each individual authorized to use ClaimsLink is issued their own ID and unique password to insure protection and to provide accountability.

Back to contents

Configuring your PC and browser

It may be helpful to print a hardcopy of these directions and check off each step as it is completed.

Minimum hardware requirements:

✎ Pentium class computer (133MHz) with 32MB RAM or better

- Video display resolution of at least 800x600 using small fonts
- 56k Modem or better (or other method for Internet connectivity)

Software requirements:
- Microsoft © Windows 98 or newer
- Microsoft © Internet Explorer 5.0 with 128 bit encryption strength or newer version of Microsoft © Internet Explorer

Medical Mutual's ClaimsLink Security Policy

Firewall
As with most organizations that supply information over the Internet, Medical Mutual uses a firewall, which forms a barrier between the Internet and Medical Mutual's internal systems. All incoming information is routed to the firewall, which verifies the source and destination of each piece of information. This way, all internal information is protected; keeping the structure of Medical Mutual's network a secret. Our firewall records all activity, including sign-ons, sign-offs, and access violations. This allows for quick identification of any suspicious activity.

Encryption

When confidential information must be sent over the Internet, the Web server ensures that it is encrypted. Encryption scrambles information so it can transfer privately from your browser to Medical Mutual's network and back. Our customers must use a browser that supports Secured Socket Layers (SSL) and 128-bit encryption for maximum protection.

Internal Controls

Strict internal procedures are in place at Medical Mutual to perform system monitoring and real-time alerting of any suspicious activity.

Back to contents

Frequently Asked Questions
What can I do to increase security?
In accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it is required that computers that display patient information be protected with a password enabled screen saver. This can be turned on using control panel from Windows XP/Vista/2007. Each customer is issued their own unique ID and associated password.

Do not share these with anyone. Make sure that no one is watching you as you enter your password. Insure that any printed identifiable health information is securely shredded. Adhere to the requirements identified in the confidentiality statement you signed. Take all possible precautions to keep your computer free from viruses that could be used to capture password keystrokes or affect your hard drive.

How do I know the encryption level my browser is using?

The encryption level you are using is determined by your browser type and version. Medical Mutual requires you to use a browser which supports North American 128-bit encryption.

How do I upgrade my browser to 128-bit encryption?

If you are not using a browser which supports 128-bit encryption, and would like to, select one of the icons below to upgrade your browser. The latest version Internet Explorer supports 128-bit encryption, which Medical Mutual requires for maximum security of online transactions. If you have questions or problems performing your upgrade, please contact the browser vendor for technical assistance.

What are Cookies?

Cookies are small data structures delivered by a web site to your hard drive. In certain cases (determined by the data in the cookie itself), the web site will require the cookie to be returned. Cookies allow a web site to store and reference a variety of information while the user is visiting their site. Cookies cannot gather data from your hard drive, get your e-mail address, or steal sensitive information.

Why does Medical Mutual use Cookies?

As most secured web sites do, ClaimsLink will deliver temporary cookies to your computer. ClaimsLink uses cookies to help ensure security. By asking for cookies to be returned, the service can verify the user requesting an action is still the same user who signed on. If your browser is configured to warn you as each cookie is delivered, make sure you accept all cookies. If you deny cookies while using Medical Mutual services, your ClaimsLink session will be terminated for your protection. While using ClaimsLink, you can configure your browser to automatically accept all cookies.

Back to contents