

## Introduction

### Background

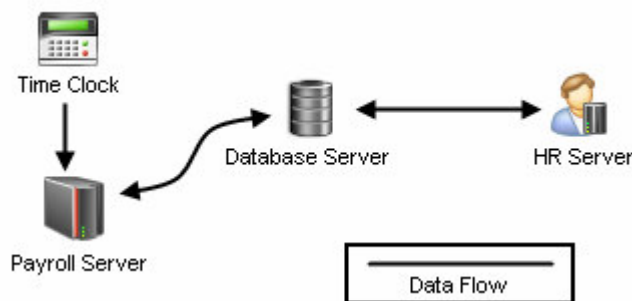
Affinity Health System is committed to protecting the privacy of its employee's personal information. While every effort is made to ensure that this information is only disclosed to authorized individuals, there is always a risk that an employee's information could be compromised. This guide is designed help employees understand how their information is stored, what happens when it is accessed, and how to protect themselves from incidental disclosure of their personal information while using the myHRaccess application.

## System Overview

### HR/Payroll System

Affinity Health System utilizes an application called myHRaccess to allow employees to access and update their personal information. This application works in conjunction with the other applications that make up the HR/Payroll system. In its most basic understanding, the system stores employee information, gathers clocking information, and calculates the paycheck.

Figure 1 is a basic overview of the components used in the HR/Payroll system at Affinity Health System.



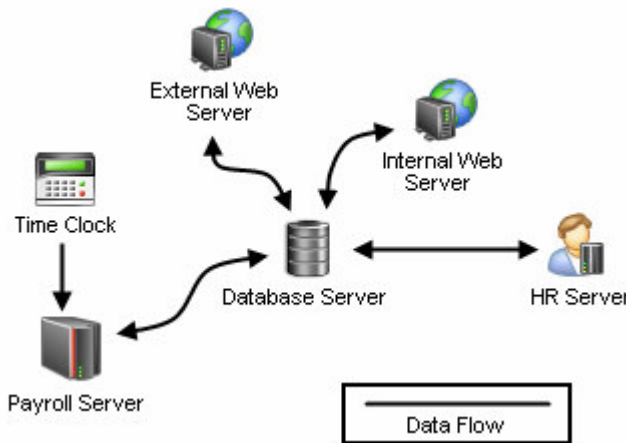
**Figure 1 - Basic HR/Payroll System Overview**

### myHRaccess Overview

myHRaccess is a web based application, meaning that it can only be used via a web browser, and is not software that is loaded on a user's computer. The application is

loaded on two servers at Affinity Health System, one to serve the internal users<sup>1</sup>, and the other serves the external users<sup>2</sup>.

Figure 2 describes how the HR/Payroll system incorporates the two myHRaccess web servers into the rest of the system.



**Figure 2 - HR/Payroll System with myHRaccess Servers**

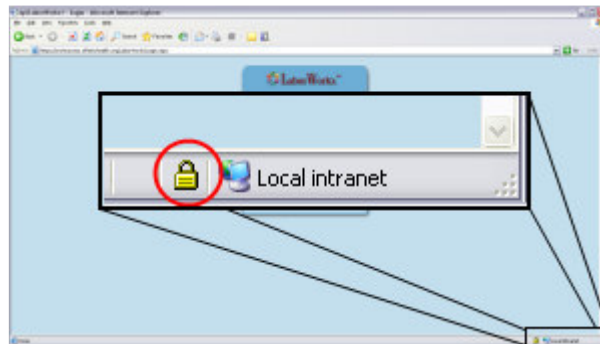
Both of the myHRaccess web servers use 128bit encryption which ensures that the data being exchanged between the server and web browser is not in an easily decipherable format. Encryption is the process of rewriting the data in such a way that only the computer with the decryption key can read it. Affinity Health System implements a public key SSL type of encryption on the myHRaccess web servers.

There is additional overhead created using encryption, as the server and web browser encrypt and decrypt the data they exchange. This will result in a noticeably slower website response time when browsing between the various items on the site.

Most web browsers will indicate a secure connection in two ways. The http:// prefix on a web address will be replaced with https://, and an icon that looks like a lock will appear. Figure 3 shows what the secure icon looks like in Internet Explorer.

<sup>1</sup> Internal users are defined as those employees accessing myHRaccess from a computer that is on Affinity Health System’s network. These are typically computers owned by Affinity Health System that are used for work purposes.

<sup>2</sup> External users are defined as those employees accessing myHRaccess from a computer that is not on the Affinity Health System network. These are typically personally owned computers, or shared computers, that are accessing the application via the Internet.



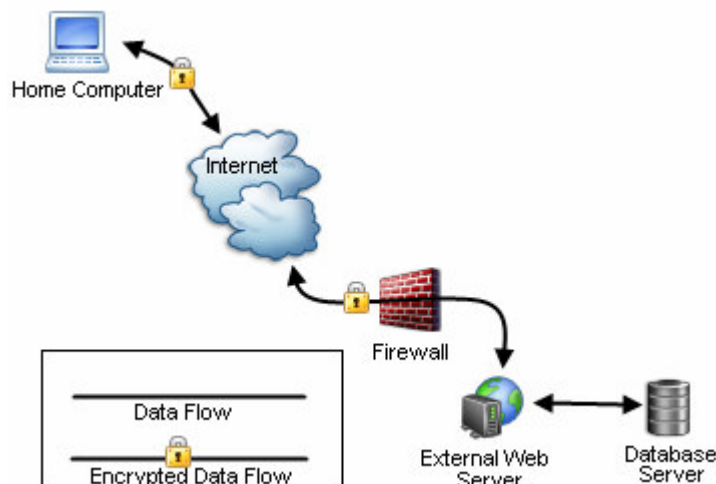
**Figure 3 - Example of a Secure Website Icon**

Additional information on how encryption works can be found at <http://computer.howstuffworks.com/encryption.htm/printable>.

### myHRaccess Data Flow

Personal information, such as address, phone number, Social Security Number, and paycheck data is only stored in the HR/Payroll system database. Upon request from a user, the myHRaccess web server queries the database for the requested information and generates a webpage to display this data in a user friendly format. Once the user logs out of myHRaccess, the information that was retrieved from the database is destroyed. Employee’s personal information is never retained on the myHRaccess web server.

Figure 4 displays a typical myHRaccess request over the Internet. The data that is sent between the home computer and the myHRaccess web server is encrypted in both directions.



**Figure 4 - Information Data Flow**



### **Internet Cache**

Most web browsers cache certain data from websites in order to make return trips to those sites faster. When a web browser caches data, it stores this data on the computer that is running the web browser. When a user visits a website that has been cached, the web browser checks to see if items on that page are newer than the items it has saved to cache. If it finds newer items, it will download those from the website, items that are the same it will load from cache. The web browser stores pictures, images, videos, scripts, and other website elements in its cache. The actual text data of the website is typically not cached because this usually changes and is the fastest part of a website to load.

While the web cache can be configured on a web browser, the website can override the web browser settings to prevent any files to be stored on the computer. Due to the sensitive information in myHRaccess, it is setup not to cache data to the computer's hard drive.

### **myHRaccess Authentication**

myHRaccess uses Active Directory authentication, which is the same authentication method that Windows uses. Domain passwords aren't stored in myHRaccess, rather myHRaccess sends the username and password to the domain and the domain returns either a success or failure indicator.

## **Best Practices and Recommendations**

### **Printing Information**

It is recommended that pay history reports and other sensitive information not be printed from myHRaccess, unless required for a specific need such as a loan application or as proof of financial income. Printing personal information increases the risk of this information being exposed to unauthorized individuals. Pay history is retained in the system indefinitely, so if a need to access previous pay history report would arise, doing so is as easy as accessing a current pay history report.

If there is a need to print a pay history report, it is suggested to use the print button located to the left of the report, and not the print icon located on the Internet Explorer toolbar. The report is formatted in such a way that it will print on one or possibly two pages, depending on the amount of information. If the Internet Explorer print button is used the pay history report will not print in the proper format.

### **Saving Information**

Information should never be exported from the system and saved. The information in the system is protected from unauthorized individuals gaining access to it, information that is saved outside of the system is not. Information that is exported from the system is not under the control of any of the safeguards currently in place to protect it, and could easily be intercepted if not properly secured.



## myHRaccess Security Guide

### **Passwords**

All of the personal information that is tied to an employee is secured in the system by that employee's password. Passwords that are weak pose a greater risk of an individual hacking into the system and gaining access to all of the information tied to that password.

Fortunately, it is not difficult to create a strong password. Strong passwords consist of at least 6 characters, and should contain a combination of letters (both upper and lowercase), numbers, and special characters (!@#%&\*^&\*()). Strong passwords also should not be a word, phrase, or name.

Microsoft provides a free password strength tool, located at:

<http://www.microsoft.com/protect/yourself/password/checker.aspx>

It defeats the purpose of a password to write it down or share it with others, and is recommended that this practice be avoided.

### **Accessing Data Externally**

myHRaccess should only be accessed from a trusted computer with proper virus scanning enabled. All computers on the Affinity Health System network are equipped with virus scan, and are trusted. Computers that are not properly protected could contain a virus or key logging software that could expose the user's username and password to unauthorized individuals.

### **AutoComplete and Remembering Passwords**

Some web browsers contain a feature to save usernames and passwords of visited websites and fill this information in automatically. It is recommended that this feature not be used with myHRaccess or any web site that contains personal information especially on a computer that is shared between multiple users.

While this feature doesn't have any affect the functionality of myHRaccess, it would allow anyone with physical access to the computer to log on as user whose credentials are stored.

### **Additional Information**

The following websites contain additional information regarding home computer security and online security.

- [http://www.cert.org/homeusers/HomeComputerSecurity/home\\_computer\\_security.pdf](http://www.cert.org/homeusers/HomeComputerSecurity/home_computer_security.pdf)
- <http://www.staysafeonline.info/>
- [http://www.cert.org/tech\\_tips/home\\_networks.html](http://www.cert.org/tech_tips/home_networks.html)

### **Copyright Information**

myHRaccess is a registered trademark of API Software Incorporated  
Windows and Internet Explorer are registered trademarks of Microsoft Corporation