
# Data Security and System for Healthcare Environment Data and Survey Software (HEDSS)

Author: John Nelson

Create Date: August 22, 2010

Last Update: November 11, 2015

Healthcare Environment, Inc.
888 West County Road D., #300
St. Paul, MN 55112

# Contents

# Introduction

Data accuracy and security is a number one priority for our customers. For online surveys, availability is crucial to accurate results. We prepared this document for you, so that you can be secure in the knowledge that Healthcare Environment Survey Software (HCESS) is up to the challenge of managing high-volume online surveys.

HCESS processes and software tools provide security and confidentiality. Our hardware configuration and high capacity network connections make certain that our web-based survey forms are reliable.

This document provides an overview of our network security practices. It also explains the separate issue of how our software provides for confidentiality. And finally why our server and network infrastructure can not only handle high demand but also can handle the kind of highly variable demand that is characteristic of large online survey processes.

# Overall Reliability

HCESS online survey and enrollment system runs in a networked environment. Security from third parties is the result of a combination of factors including the security of our network, the architecture of our proprietary software, and our policies about not disclosing client data or creating derivative works. It also complies with the HIPPA requirements.

Our accuracy results from a combination of highly reliable system availability, the architecture of our proprietary systems, and our data backup and recovery procedures.

# Software Security

## Privacy Policy

Our privacy policy ensures that the data we collect on behalf of clients remains the client's property. We do use client data in national benchmarks but do not use client names or specific information that would identify a client.

## Confidentiality

All captured data, whether electronically scanned, manually keyed or collected online, is linked to a complete audit trail that identifies the source of the data and when it was received. This system ensures complete confidentiality and accuracy. Respondent confidentiality is secured by a separation of identifying information and survey responses in our proprietary software.

For online survey processes access to the surveys or any online enrollment system is governed by the use and distribution of single, unique access codes. The survey access codes are single use.

In online enrollment systems, access is gained using a login name and password. The login name and password can be used throughout the various phases of enrollment, approval and survey administration.

This built in security in all of our web applications ensures that participants only have access to appropriate information.

## Accuracy and Quality

All of the systems we use to deliver our services are proprietary, which means we know exactly what is going on at every step of the process.

Our survey managers track and coordinate project functions for both paper and online processes. Our quality assurance and status tracking methods keep your survey administration organized, secure, accurate and on time.

HCESS is a dynamic survey system used to display surveys online and transfer responses to our data repository.

Our online survey enrollment system allows users in a multi-rater process to select their survey respondents and view the ultimate results in a confidential online environment, the HCE research portal.

## System Security

### Physical Security

The entrance to the HCE facility is either locked or attended at all times. All of our servers are secured in a locked, environmentally controlled room and are only accessible by authorized personnel.

### Network Monitoring

HCE deploys advanced security measures explained below, but any security is not worth as much if it is not actively monitored to detect attempts to break in. HCE is not a high profile target for hackers, but nonetheless we analyze our network logs to ferret out attempts to gain access to our systems. This monitoring allows us to react quickly, if needed, to deal with hackers. There are occasional attempts to break security, however none have successfully gained access to our secured internal network.

### Firewalls

A firewall is a security system that protects networks from external threats like that posed by hackers, who attempt to gain access to systems from other networks. Firewalls protect against this by preventing computers outside of HCE from communicating directly with systems on our internal network. The firewall detects attempts to gain access and both logs the activity and deflects the attacks away from internal systems.

HCE deploys a multi-tier firewall architecture which provides enhanced security through depth in our network. The first tier firewall restricts access to publicly available servers like our web servers. Then choke point firewalls restrict the access that those publicly available servers have to the rest of the network in case of the unlikely event of a system breach. Using this architecture means that even a successful attack on the initial layer of defenses does not compromise client data, which is secured behind the second layer of defenses. Combined with our network monitoring, this system has proven trustworthy.

### Secure Data Transmission

In theory, third parties could intercept client data as it passes from the survey participant's computer across the Internet to our servers. However, these types of network intercepts are difficult. To prevent any chance of intercepting your data, we use encryption that has been proven to stop possible intruders.

### Email Distribution Capacity

HCE sends email notifications at a rate that is sufficient to distribute survey notifications for most projects within a single business day. The rate for emails with attachments varies depending on the size of the attachments. Properly paced distribution of emails is important to multiple emails from the same company will not be interpreted as "mail bomb" or "Spam".

### Data integrity

In case of disk drive failure, client data remains safe and up to date as we back data up every 90 minutes and retain each days backup to ensure redundancy of dataset copies and ability to retrieve archival data. We

also protect against data loss due to catastrophe (fire, tornado, etc) by transferring backups to a secure off-site storage facility.

Data breach insurance is purchased through Hartford and is $2,000,000 per occurrence. Obtaining data breach insurance requires a rigorous review by the insurance company to ensure data integrity and security. HCE has used Hartford as an insurance vendor since 2009 and HCE has passed security review every year.

### Standards

HCE complies with the following standards/regulations:

1. Payment Card Industry – Data Security Standard (PCI-DSS)
2. HIPAA / HITECH
3. State privacy protection laws

# Summary

Overall system security results from a combination of industry accepted measures for fending off third party interlopers including physical security, network security and vigilant monitoring system activities. Confidentiality of opinion surveys, organizational, and patient data is ensured by HCESS. Backup processes and redundancy ensure data is intact despite unforeseen catastrophic events.