Sansio®

A Subsidiary of Physio-Control, Inc.

Privacy and Security Overview

Purpose

The privacy of CARES participants and patients is important to CARES and Sansio, the CARES website vendor. The purpose of this document is to give CARES participants an overview of Sansio's privacy and security practices that are applicable to the CARES software.

Sansio maintains CARES data and software in conformance with HIPAA and HITECH Act best practices. Sansio has adopted HIPAA Policies and Procedures in recognition of it's requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).

General Security Controls

1. System Architecture: CARES uses a restricted-access, secure, enterprise database, managed by Sansio.

2. Transmission Encryption: Sansio uses Secure Socket Layer (SSL) encryption technology to help ensure the integrity and privacy of the Protected Health Information (PHI). Encryption involves systematically scrambling data and is the same technology used by the banking industry and used to protect online stores. In order to take advantage of this technology, CARES participants need to have a modern web browser with updates applied that will support 128-bit encryption.

3. Data Backup: Data is protected by automated backup systems and redundant data storage.

4. Data Network Firewall: The CARES system is protected by software firewalls and intrusion prevention systems.

5. Access Controls: The system uses role-based access for all user authentication, enforcing the principle of least privilege. Control procedures are in place documenting who and how access is granted to CARES. Individual users are limited to appropriate levels of access to the data set.

Sansio's access policy combines the approaches of encryption and authentication / identification to ensure that confidential data is deliverable only to authorized parties.

6. System Timeout: The CARES web interface includes an automatic timeout after 15 minutes of inactivity.

7. De-identification: After matching EMS records with hospital outcome data, patient- identifiable information is de-identified, leaving no Protected Health Information, but allowing for statistical and demographic reporting.

Policies and Procedures:

Sansio’s HIPAA Policies and Procedures include, but are not limited to, the following:

01 General HIPAA Compliance Policy	29 Password Management Policy
02 Policies and Procedures Policy	30 Security Incident Policy
03 HIPAA Documentation Policy	31 Data Backup Policy
04 Documentation Retention Policy	32 Disaster Recovery Policy
05 Documentation Availability Policy	33 Emergency Mode Operations Policy
06 Documentation Updating Policy	34 Contingency & Emergency P&P Test & Revise Procedures
07 HIPAA Investigations Policy	35 Application & Data Criticality Analysis Policy
08 Breach Notification Policy	36 Evaluating the Effectiveness of Security P&P Policy
09 Lead HIPAA Officer Policy	37 Business Associates Policy
10 State Law Preemption Policy	38 Contingency Operations Policy
11 HIPAA Training Policy	39 Facility Security Policy
12 PHI Uses & Disclosures Policy	40 Access Control & Validation Policy
13 Patient Rights Policy	41 Facility Security Maintenance Records Policy
14 Privacy Complaints Policy	42 Workstation Use Policy
15 Risk Management Process Policy	43 Workstation Security Policy
16 Risk Analysis Policy	44 Media Disposal Policy
17 Risk Management Implementation Policy	45 Media Re-Use Policy
18 Sanction Policy	46 Hardware & Media Accountability Policy
19 Information Systems Activity Review Policy	47 Data Backup and Storage Policy
20 Assignment of Security Responsibility Policy	48 Unique User ID Policy
21 Authorization & Supervision Policy	49 Emergency Access Policy
22 Workforce Clearance Policy	50 Automatic Log- Off Policy
23 Access Termination Policy	51 Encryption and Decryption Policy
24 Access Authorization Policy	52 Audit Controls Policy
25 Access Establishment & Modification Policy	53 Data Integrity Controls Policy
26 Security Reminders Policy	54 Person or Entity Authentication Policy
27 Malware Protection Policy	55 Data Transmission Security Policy
28 Log-in Monitoring Policy	56 Mobile Device Policy