Security Standards and Procedures FAQs

This document describes the security standards and procedures that the System Coordinated Access Program directly provides or will contract to the Electronic Service Provider to protect your personal information and personal health information.

Administrative Safeguards

I. An individual(s) has been designated as being responsible for privacy and security compliance.

II. An organizational governance framework for privacy, confidentiality, and security is in place which includes clearly defined roles and responsibilities for privacy and security.

III. Organizational policies and procedures for privacy and security management have been developed and implemented, and are monitored and enforced. A mechanism is in place for reviewing and updating the policies and procedures.

IV. Only Authorized Users may have access to and use of the SCA Network for the Program in the course of performing their authorized duties and obligations.

V. Agreements are in place with all parties which contains appropriate sanctions for breach of privacy, confidentiality, or security, up to and including termination of the agreement, whatever the case may be.

VI. Nondisclosure or confidentiality agreements are in place for all employees, staff, volunteers and contractors which contain appropriate sanctions for breach of privacy, confidentiality, or security, up to and including termination of contract or employment, whatever the case may be.

VII. A privacy impact assessment and threat risk assessment have been conducted for the SCA Network. Future privacy impact assessments and threat risk assessments will be conducted as needed for the SCA Network as the electronic referral ecosystem develops.

VIII. Mandatory and ongoing (minimally annual) privacy, confidentiality, and security training is conducted for all employees, staff, volunteers and contractors using the SCA Network.

IX. A “Privacy/Security Breach” protocol has been developed and implemented. The protocol is managed by the Privacy Lead at the SCA Program Office.

X. An integrated consent management process is in place to manage and enforce Clients’ consent among participating parties. The process is managed by the Privacy Lead at the SCA Program Office.

XI. An Integrated Incident and Breach Management process is in place to detect, investigate and manage incidents collaboratively among all parties.

XII. Acceptable business recovery plans, including disaster recovery and data backup are in place.

XIII. Signed agreements have been in place with any third parties who assist in providing services related to the SCA Network, which agreements require such third parties to implement appropriate privacy and security safeguards in providing such services.

Technical & Physical Safeguards

Secure Login – Users sign in to a secure, encrypted login page. In the event that a username & password is entered incorrectly, the SCA Network uses login attempt delays, # login attempt limits, and increasingly long time-based lockout periods to prevent brute-force login attacks. Stored passwords are encrypted on the SCA Network servers (hashed & salted) – to prevent passwords from being accessed even in the event of a data breach.

Passwords – All Authorized Users are required to have secure passwords to access the SCA Network. Authorized Users do not use combinations that can be associated with them easily. Employees use highly secure passwords for accessing the SCA Network and all of supporting technology (such as servers). Passwords meet password configuration standards as per the eHealth Ontario's Acceptable Use of Information and Information Technology Policy.

Access Based on Least Privilege – This means that a user account only has privileges which are essential to that user's work. For example, a user who is responsible for processing referrals does not have access to update a clinic phone number in the listing.

Client Data Access Controls – Access to referral Client Data is strictly restricted to a) the person submitting the referral, b) the designated recipient of the referral, and c) other people within the receiving organization designated as Authorized Users to be able to view referral Client Data, in accordance with the Participant's privacy policies or any policies that CFFM provides. This is enforced through client-side encryption of private keys in a public/private key pair to ensure that only holders of a clinics encryption key can view Client Data, even in the case of a database breach.

Audit Controls – The SCA Network maintains detailed logs of logged in user activities (such as sign-ins, account modifications and accessing individual Client Data records). By request, users can view their own audit logs, and a Participant Privacy Officer or auditor can view the audit logs of all of their Authorized Users and referrals. Individual referrals clearly display the access history timeline of the referral (e.g. who booked, who received, who viewed/downloaded Client Data, who made changes). Audit logs cannot be modified.

Automatic Logoff – The SCA Network automatically logs users off of the system after a determined period of inactivity.

Secure Data Transmission – The SCA Network uses SSL 256-bit encryption when transmitting data. This is the strongest, most secure form of encryption that is generally available in Internet browsers on the market in North America today.

Firewalls – Restrictive firewall policies ensure that only approved traffic is allowed access to our servers.

Security Software Patching – Ensures that all supporting software used in the SCA Network (e.g., operating system) has the latest security updates at all times.

Secure Data Storage – In addition to the various safeguards in place to prevent access to data stored in the SCA Network, all referral personal information is encrypted so that in the unlikely event that the servers are accessed, any stolen data is useless without encryption keys.

Vulnerability Management – The SCA Network performs regular vulnerability management scans to ensure that its IT system components (OS, software) are not vulnerable to attack.

Malware Scanning – The SCA Network performs regular Malware scans to ensure its servers are clean of infected files.

Code Repository – The SCA Network use sophisticated software code management system to store and track a complete history of all code used with the SCA Network. This provides many benefits such as a) an ability to roll-back software code to a previous version in the event that a problem is found after a go-live, b) an audit trail of the SCA Network functionality at any point in time, and c) continuity of code access and availability in the event of a disaster with the Electronic Service Provider.

Physical and Environmental Security - Establish a security perimeter around the physical work environment and sensitive data processing facilities, and establish physical entry controls to reasonably ensure that only authorized individuals gain access to the environment, and environmental controls to protect against damage from fire, flood, and other forms of man-made or natural disasters.

Communications and Operations Management - Establish operating procedures and controls for the secure operations of systems and networks facilitating the access to the Confidential Information and Client Data in order to reasonably prevent accidental or deliberate misuse. Such controls include, but are not limited to, change management, least privileges granted, segregation of duties, separation of production environment from development/test environments, backups, network security, and the encryption of media in transit between Participants and Electronic Service Provider. In addition, a secure communication link (e-mail, telephony, etc.) will be maintained to ensure that Confidential Information and Client Data travelling between the parties remain secure.

Access Controls - Establish controls and procedures for the authorization, regular review and revocation of access at all levels of the system environment including physical access, network access, operating systems, applications and database access. Maintain suitable authentication controls to reasonably ensure that an individual's access rights to the Confidential Information and Client Data is appropriate for the individual's role regardless of how that individual is attempting to access that information or the location from which access is being attempted.

Information Systems Acquisition, Development and Maintenance - Maintain an application development and maintenance framework that protects the integrity of the production application and associated source code from unauthorized and untested modifications. Such a framework shall establish control over the Confidential Information and Client Data, across all environments within the development lifecycle of systems.

Incident Management - Establish policies and procedures for the timely communication and investigation of suspected breaches in the security of the Confidential Information and Client Data. At a minimum, communication of such incidents to the affected parties must take place prior to any discussion with regulators, clients, outside law enforcement agencies or representatives of the media. Incident investigations and associated information handling shall be performed in accordance with Applicable Laws.

Business Continuity Management - Appropriate policies and procedures have been established to ensure continued provision of Services.

Compliance - Policies and procedures have been established to ensure that the design, operation and management of systems and processing the Confidential Information and Client Data meets the requirements of Applicable Laws, and the requirements established in this Agreement.

Data Destruction and Disposal – Processes and controls have been implemented to ensure that any storage media or data is disposed or destroyed securely in accordance to with the reasonable requirement of SCA Program.

Auditing – SCA Program ensures vendors maintain an audit trail of the associated activities by staff or automated processes and will make available upon request any reports related to specific actions.

Security Reviews – SCA Program requests vendors conduct regular control reviews of security of their services, including, as applicable, penetration testing and intrusion detection, malware alerts, and share the results of such reviews to the applicable parties.

Internal Audit - SCA Program ensures vendors maintain adequate internal audit functions to assess internal controls in its environment, and to protect the security and confidentiality of any of the Confidential Information and Client Data which will be confirmed by the audit report. Documentation regarding internal controls will be provided upon request.

Audit Report - SCA Program requests vendors provide a report of an independent, reputable, audit firm, which report shall be compliant with the Canadian Standard on Assurance Engagements 3416 (CSAE3416) SOC 1 Type II and SOC 2 Type II Audit Reports on Controls at a Service Organization. Each report shall cover the Services for a consecutive twelve (12) month period ending March 31 in each year during the term of this Agreement. The Electronic Service Provider shall provide SCA Program with a copy of each report within thirty (30) Business Days following its receipt, which SCA Program will provide to the Participants upon request.

Workstation Use – SCA Program ensures none of their workstations store Client Data, including the workstations of the vendor's development team. All workstations are access protected with a strong password, automated timeout lock, disk encrypted & loaded with the most recent OS security patches.