CCM Data Security Control Policy

Definition
Data security controls is a comprehensive plan that encompasses users, systems, and data. Carolina Case Management (CCM) has identified numerous areas of concern in this realm and has put in policies and practices to create a secure environment for data used by CCM in normal operations.

Plan Owner
CCM IT Director

Scope
Applicable to all members of the CCM staff and all operations of the Company

Overview
Data security includes the mechanisms that control the access to and use of data at the user level. Data security policy determines which users have access to a specific object, and the specific types of actions allowed for each user on the object.

Security controls are vital to the operation of CCM. They are vital, as well, to our business partners. It is a critical operation to protect this data through appropriate measures in order to maintain the integrity and confidentiality of this information. It is clearly recognized that data can be identified in varying levels of confidentiality and thus additional measures are required in instances to protect data, but CCM must take strict steps to protect the integrity of it full complement of data.

Analysis
Data security measures will be comprehensive in nature. They are applied to users, to applications, to systems, and to physical access.

Responsibilities
The CCM IT Director, in conjunction with third party IT support group and industry sources, will define the policy for data security measures. The Director will define the controls to be applied to both user systems and network infrastructure systems. Application of these controls will be the responsibility of the IT Director in coordination with the third party IT support group and named committees within CCM.

User Groups
A tightly defined set of applications is applicable to each member of the CCM staff. These applications may vary based upon functional areas. Access to and use of these applications must be monitored and protected. For purposes of data security, five functional areas of user are defined within CCM:

1) Ownership Group
2) Management/Supervisors
3) Office Staff
4) Field Staff
5) Marketing Staff

Ownership Group
The CCM Ownership Group has access to all data within the CCM Corporation. Controls within this group is highly related to protection of the company and sensitive information.

Management/Supervisors
The management/supervisor group has access to applications that are used by the field staff, with additional access to more sensitive performance information.

Office Staff
The office staff uses data and systems to disseminate information submitted by the field staff and to support the needs of CCM customers. Data access is limited to non-sensitive status.

Field Staff
The field staff has a closely defined set of applications for use. Access levels are limited and closely monitored.

Marketing Staff
The marketing staff uses applications in conjunction with the field staff and access levels on par as well.

Applications
In normal business operations, CCM utilizes a small set of applications. The applications/Programs include both industry standard programs as well as custom applications. Access levels are as follows:

Microsoft Office
Adobe Acrobat / FoxIt
SQL Database Application (Custom Developed)
Web Browser (Edge, IE, Firefox, Chrome, Safari)

The primary control on applications is related to the SQL Database Application. This is the repository for CCM client information. Data is stored on secure Microsoft Azure servers and is web-based access. Once the application has been accessed, user credentials must be entered in order to gain entry to the database. Credentials are created and supplied by the CCM IT Director. Passwords are a combination of letters and numbers and special characters. Three unsuccessful attempts to enter a correct combination of user name and password will lock the user out of the system and prevent entry to the system until the user is reset by the CCM IT Director. Each user is assigned a role within the SQL database and this role defines the level of

data access within the program. Field case managers are given access control for data entry. Office staff receives access to view and revise data. Supervisors have access to these areas and, in addition, are able to access performance data for each of their direct reports. The ownership group has system wide access to enable code level permissions.

User Controls

Protecting data and programs that reside on personal computers is a critical task. Within CCM, all office staff is provided with desktop computers. All field personnel and supervisors are provided with laptop computers. Protecting this equipment and data that resides there is a task that CCM pursues vehemently.

The office staff is connected to the CCM LAN and most of their tasks are related to accessing the SQL database residing on Microsoft Azure servers. Thus, access must be controlled. Basic credentialing is in place for all users when accessing their desktop personal computers. This enables access to server applications. And, as noted, actual access to server applications require yet further credentialing. All of the named credentialing is assigned per user and records kept to insure privacy.

The field staff and management/supervisory staff use laptop computers. All users have been assigned boot up credentials which gives access to the programs on the computers. Barring the correct entry of credentialing information, users cannot complete the login process and are thus banned from completing access to their computer. Once on the computer, these groups will spend a large portion of their time accessing the custom SQL application residing on the CCM servers. Their access to this program requires credentialing, as noted above.

The marketing staff each are supplied with laptop computers. Their daily operation is similar to that of the field staff and their access to equipment and applications is predicated on the same controls as are assigned to the field staff via credentialing.

System Controls

CCM must start at the system level in protecting data that is vital to its operations and to its customers. A secure network has been created to for data security. Operations are centralized to a headquarters location. Onsite data storage is isolated to one server and a network attached storage device residing in the headquarters facility. Data related to the SQL Database and containing client information is stored on secure Microsoft Azure servers and resides as encrypted data in both resting and active state. Access to all servers is restricted via password protection. SQL application access is also secured via password protection. Incoming and outgoing data flow is monitored and protected by a firewall. Enterprise level anti-virus is used to protect both CCM servers. A SIEM Data Analysis system is in place to analyze incoming and outgoing data, note any outlying trends, and take/recommend appropriate actions. And, a dual system of onsite and cloud storage is deployed in the headquarters office to afford secure, redundant backup of client and company data.

Physical Access

The CCM servers and network infrastructure devices are housed in an isolated room at the CCM headquarters facility. Physical access to the equipment is limited. The CCM IT Director has full access to the room, as does approved members of the third party IT support group. All others within the CCM organization are limited in access by approval from the IT Director. CCM has installed video surveillance cameras in the headquarters office to monitor its operations. The cameras create an electronic record of any movement and the recordings can be viewed and reviewed at any time.