CCM IT Security Policy

Overview

Carolina Case Management (CCM) operations are highly dependent upon the generation, use, and successful protection of data. This data relates to all areas of the CCM operation and is considered vital to short term and long term health of the company. Securing this data and the equipment housing this data is of utmost importance to the Company.

Outline: Information Security Policy

1. Purpose
2. Goals and commitments
3. Responsibilities
4. Risk assessment and the classifications of information
5. Protection of information systems and assets
6. Protection of confidential information

1. Purpose

This policy defines a plan for the management of information security within the CCM organization. This policy applies to all internal users, third party support groups, and any organizations/individuals that interact with the CCM systems.

2. Goals and Commitments

2.1 CCM clearly recognizes the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems are essential to the normal and everyday operation of the company and the long term viability of the Company.

2.2 Damage to network infrastructure and/or computing equipment, along with the associated data, can have dire financial consequences for the Company. Protection of said equipment and data is vital.

2.3 To mitigate these risks, IT security must be an integral part of information management, whether the information is held in electronic or hard-copy form.

2.4 CCM is committed to protecting the security of its information and information systems in order to insure that:

1. The integrity of information is maintained to insure accuracy.

2. Information is always available to those who need it and there is no disruption to the CCM business.
3. Confidentiality is not breached.
4. The reputation of CCM is safeguarded.

2.5 Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

2.6 CCM is committed to providing sufficient education and training to users to ensure they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information. Users will be identified by CCM for such education and training, with the education and training being sufficient for their "need-to-know" levels.

2.7 CCM will establish and maintain appropriate contacts with other organizations with regard to IT security policies as it affects them and as these policies need to be distributed.

2.8 Breaches of information security must be recorded and reported to the CCM IT Director. Appropriate and swift actions will be taken to resolve resultant problems and to prevent future recurrence.

2.9 This Policy and all other supporting policy documents shall be communicated as necessary to appropriate personnel with the CCM organization.

3. Responsibilities

CCM Ownership Group

3.1 The CCM Ownership group has the ultimate responsibility for creation and execution of the CCM IT Security Plan. Application of the plan is the responsibility of the CCM IT Director, who will work with assigned personnel to disseminate the information throughout the organization.

Users and External Parties

3.2 Users of CCM information will be made aware of their own individual responsibilities for complying with CCM policies on information security.

3.3 Agreements with third parties involving accessing, processing, communicating or managing CCM's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

4. Risk Assessment / Information Classification

4.1 Security levels are a function of assessing the value, vulnerability, and accessibility needs of systems and data. Therefore, a risk assessment is required in this realm in order to identify and classify the nature of the information held, the adverse consequences of security breaches, and the likelihood of those consequences occurring.

4.2 Risk assessments will be coordinated by the CCM IT Director. The IT Director will name any personnel or outside third party organizations who are needed to be a part of and complete risk assessments related to systems and information.

4.3 The risk assessment will assets; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to the Company

4.4 Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

4.5 Rules for the acceptable use of information assets should be identified, documented and implemented per the direction of the CCM IT Director.

4.6 Information security risk assessments should be repeated periodically to insure up-to-date evaluations on systems and information in use by the Company.

4.7 Personal data, whether related to internal CCM employees or clients being managed by the Company must be handled with the goal of strict confidentiality. This information must be protected at all times.

> Internal Documentation. Personnel records and data will be stored hard copy in the office of the CCM IT Director. These documents will be stored in locked filing cabinets and the keys will be kept confidentially by the Director. Any electronic copies will be stored on CCM servers in folders with clearly assigned permission levels. Permissions to access these folders will be limited to the Ownership Group and any personnel specifically identified by the IT Director.

Client Documentation. Client documentation will reside in the CCM Bluenotes application (SQL Database Application). Access will be limited and restricted per user level and password protected per Company Policy (see CCM Password Policy).

5. Protection of Information Systems and Assets

5.1 Having completed a risk assessment of assets, CCM will take appropriate steps to insure the security of said assets in accordance with their deemed value and vulnerability.

5.2. Confidential information should be handled in accordance with the requirements set out in section 6 below.

5.3 All new hires will be instructed and trained at new hire orientation regarding importance and key practices of protecting assets and information of CCM. This training will cover best practices for protecting equipment as well as CCM policy for use of equipment and accepted principles to insure protection of all data.

5.4 Upon termination of an employee, the supervisor of the terminated employee will work to insure the removal of said employee from CCM systems as well as collection of CCM assets, i.e. computing equipment, phones, files, etc. Unless otherwise requested, employee will be removed as a login user from CCM systems within 48 hours of termination.

6. Protection of Confidential Information

Identifying confidential information is critical. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorized disclosure could have one or more of the following consequences:

1. financial loss
2. reputational damage
3. an adverse effect on the safety of members of the CCM organization or its partners.

6.1 Storage

6.1.1 Confidential information will be kept secure, using, where practicable, dedicated storage (e.g. file servers) rather than local hard disks, and an appropriate level of physical security.

6.1.2 File or disk encryption should be considered as an additional layer of defense, where physical security is considered insufficient.

6.2 Access

6.2.1 Confidential information must be stored in such a way as to ensure that only authorized persons can access it.

6.2.2 All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined policies should be in place and implemented. Users must follow CCM mandated security practices in the selection and use of passwords, as outlined in the CCM Password Policy Document.

6.2.3 Where necessary and deemed appropriate, additional forms of authentication will be considered.

6.2.4 Physical access should be monitored, and access records maintained.

6.3 Remote access

6.3.1 Where remote access is required, this must be controlled via a well-defined access control policy and tight access controls provided to allow the minimum access necessary.

6.3.2 Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

6.4 Copying

6.4.1 The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where necessary, a record kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed (see 6.12.5).

6.4.2 All copies should be physically secured e.g. stored in a locked cupboard drawer or filing cabinet.

6.5 Disposal

Policies and procedures must be in place for the secure disposal/destruction of confidential information.

6.6 Use of portable devices or media

6.6.1 Procedures should be in place for the management of removable media in order to insure that they are appropriately protected from unauthorized access.

6.6.2 The permission of the information owner should be sought before confidential information is taken off site. The owner must be satisfied that the removal is necessary and that appropriate safeguards are in place e.g. encryption/password protection.

6.7 Exchange of Information and use of Email

6.7.1 Controls should be implemented to ensure that electronic emailing is suitably protected.

6.7.2 Email should be appropriately protected from unauthorized use and access.

6.7.3 Email should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken.

6.8 Password controls

6.8.1 Procedures should be in place to support the use of password techniques and to ensure that only authorized personnel may gain access to confidential information. Ref: CCM Password Policy Document.

6.9 Backup

Information owners should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken and tested regularly in accordance with such an appropriate backup policy.

6.10 Hard Copies

Protective marking

6.10.1 Documents containing confidential information must be marked as 'Confidential'.

Storage

6.10.2 a. Wherever practicable, documents with confidential information should be stored in locked cabinets. Locations of confidential information must be clearly known and access limited to those who are approved to access and view such documents.

6.10.2 b. Keys to cabinets should not be left on open display when the room is unoccupied.

Removal

6.10.3 Confidential information should not be removed from the CCM offices unless it is being destroyed. Exception is the need for such information by the CCM Ownership Group.

Transmission

6.10.4 a. If confidential documents are sent by fax, the sender should insure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

b. If confidential documents are sent by external post, they should ideally be sent by a form of recorded delivery. The sender must insure that the envelope is properly secured.

c. If confidential documents are sent by internal post the documents should be placed in an envelope marked 'Confidential' with the addressee's name clearly written on it.

Disposal

6.10.5 Confidential documents must be shredded in a confidential manner prior to disposal.

6.11 Enforcement

6.11.1 All members of the CCM staff and any associated third party providers are bound to work within the parameters of the CCM IT Security Policy. Any known violation of the policy must be reported to the CCM IT Director. Appropriate actions will be taken by the Director to resolve issues and to insure no future reoccurrence of the violation.