

Policy Manual

Subject: Security in Outsourcing and Contracts

Section: ADM – Legal Issues

Number: ADM-c-130

Approved: Chief Executive Officer

Date: 004.05.15 R05.06.15

POLICY

This policy covers the protection of health information accessed or held by outsourcing and other third parties on behalf of CapitalCare. It includes security of information technology (IT) systems managed and/or controlled by service providers. Third party access to information management / processing facilities or information assets includes, but is not limited to, access by:

- IT hardware and software vendor maintenance and support staff
- Consultants
- Business partners
- Support services such as security guards, cleaning or catering contractors
- Student placements or volunteers

PROCEDURE:

1. Risk Assessment of Outsourcing and Third Party Access

- 1.1. A risk assessment is required prior to entering into an agreement with a third party where health information is involved. The Security and Confidentiality Officer of Capital Health will carry out risk assessments related to information technology (IT) systems and the Manager of Materiel Management will carry out risk assessments related to other services. Risk assessments will identify the security and privacy infrastructure of third parties for outsourced or contracted functions, and recommend appropriate security controls.

- 1.2. Until recommended security controls are implemented, and a contract executed with explicit access provisions, the third party must not allow access to premises or systems containing health information by other third parties.
- 1.3. Risk assessments in response to requests for physical access to facilities or logical access to databases by third parties will be performed.
- 1.4. If a Privacy Impact Assessment is required for the initiative, it must be accepted by the Office of the Information and Privacy Commissioner prior to access being granted (see Policy ADM-c-180).

2. General Contract Provisions for Information Security

- 2.1. Third party security provisions in contracts must meet or exceed CapitalCare's Information Security Policies and related procedures. Any related third party information security and privacy policies will be made available to CapitalCare, including updates or revisions that occur after execution of the contract. CapitalCare will retain the right to inspect third party premises and security practices to ensure compliance with contract provisions and stated policies.
- 2.2. Contracts will document third party roles and responsibilities for carrying out specific security processes. Security responsibilities regarding hardware, software, network, applications and data must be defined and incorporated into the contract. Third parties must provide an organizational chart that shows the positions responsible for the operational implementation of security policies, and a contact name for support in dealing with breach investigations. CapitalCare will require contracted third parties to report breaches of confidentiality and privacy according to CapitalCare procedures, within agreed time constraints.
- 2.3. Contracts with IT Service Providers or other third parties must include provisions that protect CapitalCare operations from failures that are a direct result of the inability of the provider to meet contract requirements. In order to mitigate these situations, disaster recovery and system backup must be included in all agreements, to a standard that meets or exceeds that of CapitalCare.
- 2.4. Third parties accessing CapitalCare systems will be subject to predefined periods of authorized use and have limited default access. Additions or extensions to third party access must be approved before access is granted to the individual. All external network access requirements for third parties will be provided through a controlled access point, without exception, definition of which will be included in the contract.
- 2.5. Capital Health's Security and Confidentiality Officer and the HIA Coordinator must be notified of potential requirements for third party access to systems before the introduction of new products or business initiatives. If required, a Privacy Impact Assessment will be completed in accordance with Policy ADM-c-180.
- 2.6. CapitalCare will retain the right to access information assets in the custody of third parties within 48 hours of submitting a request for access. Third parties may not

deny access to, or retain custody of, confidential information requested by CapitalCare because of late or disputed payment for services.

- 2.7. Third party and outsourcing contracts must include provisions for ensuring that employees of the contracted party are aware of, and familiar with, CapitalCare's health information and security policies.

3. Out of Province Contracts

- 3.1. Prior to the use, disclosure or storage of health information outside of Alberta, CapitalCare will enter into a written agreement with the person who is to use, store or have disclosed to them health information. The agreement will:

- Provide for CapitalCare to retain control over the health information
- Adequately address the risks associated with the storage, use or disclosure of the health information
- Require the person to implement and maintain adequate safeguards for the security and protection of the health information,
- Allow CapitalCare to monitor compliance with the terms and conditions of the agreement, and
- Contain remedies to address any non-compliance with or breach of the agreement by the other person.

- 3.2. This section does not apply to health information about an individual that is used solely for the purpose of providing continuing treatment and care to that individual.

4. Outsourcer and Third Party Responsibilities Reflected in Contracts

- 4.1. Outsourcers or other third parties will not grant access to CapitalCare information systems or assets in their custody until approval has been granted by CapitalCare (or by the IT Service Provider or Third Party under delegated authority of CapitalCare).
- 4.2. Third parties and outsourcers will ensure that the termination process for employees includes return of, and revoking of access rights to, all information assets, applications, hardware, software, network and facilities of both the contracted party and CapitalCare.
- 4.3. Third parties and outsourcers will protect CapitalCare information and systems from damage or misuse by any person or organization.
- 4.4. Third parties and outsourcers will work with Capital Health's Security and Confidentiality Officer (in the case of IT systems) or the Manager of Material Management (in the case of other services) as required to implement an annual security review and address any threats to security identified by the audit.

- 4.5. Third parties and outsourcers will destroy or return all CapitalCare owned hardware, system, documentation and information assets upon termination of agreements and in accordance with contract provisions reflecting records and data management policy.
- 4.6. Third parties and outsourcers will inform their employees at the commencement of employment about requirements to adhere to CapitalCare security and privacy/confidentiality policy for those with access to CapitalCare information assets or systems.
- 4.7. Third parties and outsourcers must remind their own employees on termination of their continued responsibility to maintain the confidentiality of CapitalCare information.

5. Enforcement of Information Security Contract Provisions

After an agreement or contract has been executed for third parties who require access to information systems and assets of CapitalCare, compliance with security contract provisions will be continually monitored and enforced.

- 5.1. Contractors will be requested to sign and acknowledge receipt of current and updated Information Security Policies they are bound to follow under contract.
- 5.2. Information Systems will actively monitor third parties and outsourcers with access to CapitalCare information assets or systems for inappropriate access or use.
- 5.3. Third party access requirements will be reviewed on a regular basis for required changes.
- 5.4. Third party and outsourcer information processing or storage facilities will be inspected to ensure compliance with all security provisions and policies.