

PLAIN LANGUAGE DESCRIPTION OF CARECHAIN AND SECURITY SAFEGUARDS

This statement was updated on December 18, 2022.

OVERVIEW

The following is a plain language description of CareChain and security safeguards used by MultiCIM Technologies Inc. ("**MultiCIM**"). This description provides an explanation to health care providers and the public who use CareChain. It explains how privacy and security processes in place will ensure the confidentiality of the Personal Information and Personal Health Information (collectively referred together as "**Information**") used in the provision of such services.

DESCRIPTION OF CARECHAIN

CareChain is a health care management platform provided by MultiCIM that enables independent, regulated health care providers to: (i) receive and fulfill requests for health care services; (ii) manage patient records; (iii) initiate appropriate patient referrals to other health care providers in the CareChain network; and (iv) exchange relevant patient records with other independent, regulated health care providers to facilitate health care services.

CARECHAIN SAFEGUARDS

MultiCIM provides the following administrative, physical and technical controls to enable health care providers using CareChain ("**CareChain Providers**") to disclose Information to one another:

Administrative controls

- Appointed a senior member of the leadership team to act as the executive point of accountability.
- Agreements, policies, and procedures define each party's role in protecting Information when using CareChain. They also define the roles of any people working for MultiCIM or CareChain Providers.
- Provides incident and breach management support to CareChain Providers and has an established privacy incident and breach management protocol within MultiCIM.
- Privacy and security assessments are conducted to identify new risks to privacy and security when MultiCIM believes that there is a significant change to CareChain or the collection, use and/or disclosure of Information within CareChain or MultiCIM.
- Notifies CareChain Providers of any unauthorized access to Information that the CareChain Provider enters into CareChain.
- Conducts audits on behalf of CareChain Providers to comply with legislative requirements and ensure appropriate access to Information.

Physical controls

- Facilities are physically protected against unauthorized access and are staffed and monitored continuously by security staff and affiliates.

- When servers are no longer needed, the hard disks storing the Information are physically destroyed or permanently erased.
- Information is not physically removed from the data centre.
- Backup systems are in place to protect against environmental issues such as power outages or hardware failures.

Technical controls

- Implemented authorization and authentication controls to limit access to Information only to those individuals who require it to perform their job function.
- Everyone needs a password to access CareChain and Information.
- All data is transmitted via a secure encrypted channel.
- The network is monitored to identify anyone trying to hack into it.
- All actions in the information system are logged so that it can be monitored and audited.

CONTACT US

If you have any questions, concerns or suggestions about our privacy practices, please contact our Privacy Officer. Please include your name and contact information if you'd like us to respond to you.

ATTN: Privacy Officer

privacy@carechain.app