Information Security Policy

Crowfoot Physio takes the security and privacy of your information seriously. We are committed to ensuring that the technology we use maintains the security of your personal and health information.

Crowfoot Physio uses Jane Software for clinic management and electronic medical records. All patient information is stored in Jane, using Jane servers. Patient information such as communications and reports may be stored on local computers, networked on site, and backed up to an external hard drive at regular intervals. In this policy we will discuss the security of both Jane and the on-site technology. Telehealth sessions will be conducted via PhysiTrack or telephone on encrypted wifi on personal devices.

Should Crowfoot Physio change electronic medical records systems, this would trigger a PIA to ensure confidentiality, integrity, or availability of health information.

Jane Security

Patient data (charts, patient profiles, appointment history etc) is always owned by Crowfoot Physio. So what that means is that Jane acts as an agent storing patient data on behalf of their customers. Crowfoot Physio retains ownership of all patient data.

Jane Data is stored on two secure servers on proper data centres, both located in the Montreal area.

All servers are SOC2 certified at a minimum, which means that only authorized individuals have access to the facilities.

Jane Data is encrypted using 256 bit encryption when sent between your device and our servers (in the same way as your banking information would be).

Administrators, practitioners and patients each access Jane using their own account secured by a username and password. Account owners can control access permissions for each user, which includes control of accessing patient charts, billing records, and schedule records.

Jane uses mirrored database servers (which act as real-time backups) so in the unlikely event that something happens in data centre, Jane can flip over immediately to use the other database server. Jane also performs nightly off-site backups, just as an additional precautionary measure.

Jane offers a user-activity report to account owners in which they can see a detailed breakdown of all user activity. The report can be filtered by date range, user, and type of access for regular reviews on who is accessing patient charts.

On-Site Security

All on-site computers and computers used for telehealth appointments are equipped with Antivirus and Malware software (Windows Security Essentials and CCleaner). Firewalls and Intrusion Detection is included on all computers by Windows Firewall.

Any patient information that is transferred via email to a third party must be sent in a password protected and encrypted email.

On-site computers are backed up monthly to an external hard drive which is password protected and stored in a secure location.

All computers are equipped with passwords to access the computer and timed lock screens. Computers are stored in secure areas, separate from patient treatment areas. Any computers used for telehealth appointments are personal devices, not shared. They are stored in secure areas and require the same security requirements as all on-site computers. Fax machines, copiers, and other office equipment is also stored in secure areas, separated from patient treatment areas.

Security Policies

As agreed upon in the Jane Terms and Conditions, files and other content in the services may be protected by intellectual property right of others. Crowfoot Physio agrees to not copy, upload, download, or share files unless we have the right to do so. Crowfoot Physio, not Jane, will be fully responsible and liable for what we copy, share, upload, download or otherwise use while using Jane. Crowfoot Physio must not upload spyware or any other malicious software to the Jane.

All users are responsible for safeguarding the password used to access Jane and agree not to disclose the password to any third party. Each user is responsible for any activity on their account, whether or not they authorized that activity. Users should immediately notify Jane of any unauthorized use of the account.

All users must update their passwords quarterly to maintain security.

If Jane is being accessed remotely, each user is responsible for ensuring the device being used to access Jane has appropriate anti-virus, malware, firewalls, and intrusion detection.

Once logged in, every click of every button is tracked for each user. Clinic owner and Privacy Officer can audit the user's Activity Log in Jane and view all activity for all users or filter the report to see what health information a particular staff member accessed over a specific time frame.

Access to Jane is immediately revoked upon termination of an employment agreement or contract.

Any breaches in security should be addressed by the Privacy Incident Response Policy and Procedure.

Staff Training

All staff undergo initial privacy and security training performed by the Privacy Officer. Each staff member must sign a Privacy Agreement prior to being granted access to Jane.

On a quarterly basis, all privacy policies are reviewed by the Privacy Officer. Each staff meeting includes a time to discuss privacy and security issues as determined by the Privacy Officer. Should this review so indicate, a PIA may be triggered and performed by the Privacy Officer or appropriate custodian.

Privacy Accountability

Our Privacy Officer, Beverly Landry, is responsible for implementing and maintaining our Privacy Policies. Beverly is also the Clinic Administrator for Crowfoot Physio. Beverly Landry will complete all training with new staff members and facilitate the quarterly review and training at staff meetings.

In the case of any Privacy Incidents, Beverly Landry, in conjunction with the Clinic Owner, Tim Kutash, a thorough investigation and follow-up will be completed.

In the case of any requests for Health Information, a request form should be submitted to Beverly Landry and, in conjunction with the appropriate clinician, she will follow-up with the request.

All front desk staff are responsible for maintaining the accuracy of health information. All staff are responsible for protecting confidentiality and to collect, use and disclose health information in a limited manner.

Joshua Kim is responsible for ensuring all technical and administrative safeguards are in place on all on-site computers as well as providing guidance and direction for telehealth procedures.