[PAGE 1]

E-Stroke Privacy and Security Program

The E-Stroke Solution is a shared web-based system containing personal health information in the form of referrals. The system supports efficient inpatient and outpatient rehab referrals for stroke patients between all acute care and rehab hospitals in Toronto. It also tracks demand, wait times, response times and other indicators in order to measure and evaluate access and system efficiency. As of 2008 in the Toronto Central LHIN clinicians involved in the client's care in acute care and rehabilitation facilities are able to access data in E-STROKE and view the personal health information in referrals sent by or received by their organization. See below for a list of participating organizations and the types of personal health information being captured in the information system.

How is Patient Health Information Used and Protected?

Patient's referral information is made available to patient selected healthcare organizations for the purpose of providing the patient with healthcare and treatment. All healthcare organizations involved in the E-Stroke solution handle a patient's personal health information securely and confidentially, in accordance with Ontario's health privacy law (Personal Health Information Protection Act, 2004), other applicable laws, and the E-Stroke and Security Policies and Procedures.

Who Operates the E-Stroke Program?

The University Health Network (UHN) operates the E-Stroke Solution on behalf of the Toronto Stroke Networks and provides the technical services that allow personal health information to be shared electronically by:

- Managing and operating the E-Stroke program and information system;
- Assessing the privacy and security of the information system to help ensure that it protects personal health information;
- Operating the E-Stroke Privacy and Security Program in cooperation with participating healthcare organizations, including communicating directly with individuals about privacy or security questions or complaints;
- Developing and managing some of the technology needed to support the information system; and
- Managing service providers who built and support the information system.

When the University Health Network provides these technical services, it has access to the personal health information in the information system. It only uses personal health information to perform these services to healthcare organizations and does not disclose the personal health information to any other healthcare organizations.

The University Health Network is also a healthcare provider organization that will be able to view personal health information to provide treatment and care like any other healthcare organization that is participating.

Patient Privacy Rights

Patients can contact E-Stroke or any healthcare organization participating in E-Stroke for any privacy and security questions or complaints. Please refer to the contact information at the end of this page.

A patient would likely contact their healthcare organization for the following privacy-related reasons:

Consent and Blocking a Patient Record

Healthcare organizations may use and share patient personal health information for treatment and care. All healthcare organizations that use and share patient personal health information in the information system have signed agreements confirming that they follow E-Stroke's Privacy and Security Policies and Procedures and Ontario's health privacy law.

The electronic referral system (E-Stroke) is the standard of care to access rehabilitation in Toronto. Personal health information is required to make decisions on rehabilitation applications. After a referral has been sent your personal health information will be reviewed by staff at the receiving organization to make a decision about your rehab application.

Patients can choose to not have their personal health information shared with other healthcare organizations through this system. This needs to be done before the referral is made. Patients who would like to have their referral information restricted should tell their care provider before the referral is made.

Viewing or Obtaining a Copy of Personal Health Information

Patients have a right to request to see or obtain a copy of the following:

- The patient's personal health information in the information system
- A list of healthcare professionals who have viewed a patient's personal health information in the information system

Patients who would like to view or obtain a copy of their information in E-Stroke should contact their healthcare organization to make the request.

Correcting Personal Health Information

Patients have a right to ask that their personal health information be corrected if they feel it is out-of-date or inaccurate. Patients who would like to make a correction to their information should contact their healthcare organization to make the request.

Questions or Complaints about E-Stroke's Practices

Everyone has a right to ask questions or make a complaint about how E-Stroke handles personal health information or privacy. Individuals who would like to ask a question or make a complaint about E-Stroke's practices can do so either to their healthcare organization or directly to the E-STROKE program.

Contact Information

The most secure way to contact E-Stroke is by phone or mail. Patients may choose to email E-Stroke, but the security of email messages is not guaranteed. Messages may be forged, forwarded, or seen by others using the internet. **Please note:** Patients should not use email to discuss sensitive information, or use email in an emergency since it may be delayed.

Telephone: 416 340 4800 ext. 6937

Mailing Address:

E-Stroke Privacy Office
c/o E-Stroke Program Office
University Health Network
20 Dundas Street West, 3rd Floor
Toronto, ON M5B 1R4
Emailprivacy@uhn.ca

Personal Health Information in the E-Stroke Solution

The following types of information are stored in the information system. This list will be updated from time to time as new types of information are added into the information system, but may not represent a complete list of all types of PHI captured through the E-Stroke Solution.

Not all of the healthcare organizations using E-Stroke provide all of the information described below. Some may only provide some of the personal health information types.

Personal Health Information Type	Description or Examples	Purpose of Storing the Personal Health Information
Demographics	• Name • Gender • Health Card Number Information • Supplementary Health Card Information • Client ID relevant only to the E-Stroke system • Date of Birth • Marital Status • Patient Phone Number • Permanent Address (including postal code, telephone number) • Next of Kin • Medical Record Number • Premorbid vocational status	Identify patient and link their personal health information from multiple healthcare organizations
Patient Social Information	• Social Situation Details • Living Situation • Preferred Accommodation • Emergency Contact • Alternate Contacts (POA Personal Care and Financial Affairs, SDM, non-legal contacts) • Primary Language • Interpreter Required • Preferred Language •	Providing treatment and care
Financial Information	• Health Insurance Information • Responsibility for Payment (e.g. OHIP, Insurance Plan)	Providing treatment and care
Health Care Provider Information	• Physician Information (Hospital) • Family Physician Information (Community) • Referred by Information	Ability to acquire more patient information to provide treatment and care
Relevant Medical History	• Precautions/ Risks (to patient and/or provider) • Conditions Impacting on Rehab Potential • Pre-existing Medical Conditions • Surgical History	Providing treatment and care

	• Psychiatric History • History of Falls Information	
Current Condition	• Physical and Mental Health, Surgical, Family, Social Condition • Drug Sensitivities, Allergies, Addictions • Infection Control • Current Treatments/ Special Needs • Current Diet • Vision Information • Hearing Information • Speech Information • Mobility/ Ambulation Information • Height • Weight	Providing treatment and care
Relevant Diagnosis	• Primary Diagnosis of stroke and relevant information (e.g. type of stroke, mechanism of stroke, deficits current and prior if applicable, completed stroke workup and medical imaging information) • Co-morbidities	Providing treatment and care
Visit/ Encounter Details	• Admission date • Discharge date • Discharge destination at time of discharge • Date of Referral • Service Requested (e.g. inpatient or outpatient rehab) • Goals of Care (e.g. rehabilitation goals) • Client Choice Information • Special Care Needs	Providing treatment and care
Allied Health Information	• Nursing Intervention Information • Occupational Therapy (functional status, suggested goals, progress) • Physiotherapy Report (functional status, suggested goals , ambulation details, progress) • Social Work Intervention Information • Speech Language Pathology Information (communication and/or swallowing disorders, hearing, assessments, therapy)	Providing treatment and care
Mental Health and Addiction Information	• Psychiatric History	Providing treatment and care
Special Care Needs	• Safety –risk of falls/wandering and support required • Tracheostomy • IV • Oxygen • Enteral Feed • Dialysis • Skin Condition • Infection Status and Needs • Equipment Needs	Providing treatment and care

	• Bladder Management • Bowel Management • Ostomy • Feeding Requirements • Dietary Needs	
Assessments	• Behavioural findings • Symptom Assessment (Edmonton Symptom Assessment System score) • Functional Assessment • Stroke Severity Assessment • Cognitive Status (Montreal Cognitive Assessment or Mini Mental State Examination) • Ambulatory Status	Providing treatment and care

More Questions?

For more information on E-Stroke Privacy and Security, please contact us.

[PAGE 3]

E-Stroke Participating Organizations

Sector	Organization Name
Acute Care and Rehab	Bridgepoint Health Humber River Hospital Michael Garron Hospital Mount Sinai Hospital North York General Hospital Providence Healthcare Rouge Valley Health System St John's Rehabilitation Hospital St Joseph's Health Centre St Michael's Hospital Sunnybrook Health Sciences Centre The Scarborough Hospital Toronto Rehabilitation University Health Network West Park Healthcare Centre

Keeping Personal Health Information Confidential and Secure

The E-Stroke Program keeps personal health information safe with controls including:

Administrative Controls

- The E-Stroke Advisory Committee (made up of the healthcare organizations participating in E-Stroke) oversees the privacy and security programs.
- Privacy and Security Leads for the E-Stroke Program ensure that there are privacy and security programs in place to protect personal health information.
- Healthcare organizations must ensure that their healthcare providers are informed of their duties.
- Agreements, policies, and procedures define each organization's role in protecting the personal health information. They also define the roles of any people working for the organization or service providers who provide the healthcare organizations with services.
- Privacy and security assessments are conducted to identify new risks to privacy and security when the Privacy and Security Working Group or E-Stroke Executive Committee feels that there is a significant enough change to the E-Stroke Program or information system.
- The E-Stroke Program notifies healthcare organizations of any unauthorized access to personal health information that the healthcare organization put in the information system.

Physical Controls

- The personal health information is stored in a data centre with cameras, restricted access, alarms, and 24/7 security.
- When servers are no longer needed, the hard disks storing the personal health information are physically destroyed or permanently erased.
- Information is not physically removed from the data centre.

Technical Controls

- Only approved healthcare providers and staff that support them can view the information.
- Everyone needs a password to access the personal health information.
- The actions of everyone who views the personal health information is recorded electronically.
- 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 the privacy officers of the healthcare organizations are able to monitor and audit their healthcare providers and staff who view personal health information in the information system.