OPHRDC
The Ontario Physician Human Resources Data Centre

209-565 Sanatorium Rd.
Hamilton, ON L9C 7N4
(905) 296-4811 ext. 505

OPHRDC Data Privacy and Security

The following summary contains excerpts from the full policy document OPHRDC Data Management Policies and Procedures, draft version, 13AUG2019.

Introduction

The Ontario Physician Human Resources Data Centre (OPHRDC) provides this summary to make you aware of our privacy policy and practices. OPHRDC regards access to personal information as an important privilege and we are committed to protecting the privacy of all personal information that we collect.

Personal Information means "information about an identifiable individual" (Digital Privacy Act – 2015, c.32 (Section 2), Government of Canada). Any published information or reporting is for statistical purposes only and OPHRDC does not publish or provide identifiable data to any third parties without consent of the organization that has shared this data with OPHRDC.

OPHRDC is bound by the Freedom of Information and Protection of Privacy Act, the Personal Information Protection and Electronic Documents Act (PIPEDA), as well as the data sharing agreements and memorandums of understanding that OPHRDC has with their partner organizations:

- Ministry of Health and Long-Term Care (MoHLTC)
- College of Physicians and Surgeons of Ontario (CPSO)
- Ontario Medical Association (OMA)
- Council of Ontario Faculties of Medicine (COFM) [includes each of the six Ontario medical schools]

All OPHRDC staff are aware of the need to keep confidential any personal information that comes to their attention in the course of their duties, except when the information is widely and publicly available. All of OPHRDC's employees must sign McMaster's Confidentiality Agreement as a condition of employment.

Data Holdings

The information we retain about physicians practicing or training in Ontario includes:

- Identifier Information (for internal purposes only)
- Medical Information Number for Canada (MINC)
- Demographic Information (age, gender, citizenship, DOB)
- Specialty Information (certified specialties, year obtained, focused areas of practice)
- Licensure (status, year obtained, expiry date)
- MD information (location, year)
- PG information (university, location, year, language, source of funding, training status, program of training, start/end dates, full-time or part-time)
- Primary Practice information (location, full-time or part-time)

- Hospital appointments or rotations
- Canadian Residency Matching Service (CaRMS) data

This data is used in the following databases:

DATABASE	SOURCE DATA	Annual Reports Published (no identifiable information)	Identifiable Reports Not Published but Provided to following organizations
Active Physician Registry (APR)	CPSO, PHAL, Dynamic Physician Survey, PG, OMA, MoHLTC	Physicians in Ontario (PIO), multiple special reports	MoHLTC, OMA
Physician Hospital Appointments Listing (PHAL)	Ontario hospitals		MoHLTC (via APR)
Ontario Postgraduate Registry (PG)	Ontario medical schools (CaRMS data)		Ontario medical schools, CPSO, PARO
	Ontario medical schools (PG registration data}	Postgraduate Medical Trainees in Ontario (PMTIO), other special reports	PARO, CAPER, MoHLTC,
Medical Trainee Days (MTD) Database	Ontario medical schools in collaboration with Ontario hospitals [verified with CPSO and MINC data]		MoHLTC [quarterly and annual]

Data Privacy

Any published information or reporting is in aggregate form for statistical purposes only. OPHRDC does not publish or provide identifiable data to any third parties without consent of the organization that shared this data with OPHRDC. When physician-specific information is disclosed to one of our partner organizations, it is always done through our secure File Transfer site.

Aggregate reports are prepared for other interested parties on request but never include uniquely identifiable physician data. This type of information may be transmitted by e-mail.

OPHRDC does not use any personal Information collected for commercial purposes.

Physician's Right to Access their Own Information

OPHRDC makes every effort to ensure that the physician information that we collect is sufficiently accurate, complete and up-to-date to meet our reporting purposes.

Subject to applicable legislation, any Ontario physician can request access to their own information maintained in OPHRDC's database. They can also request that their information be corrected/ updated by contacting OPHRDC directly (see contact information below).

Data Security

OPHRDC takes every measure to prevent unauthorized access and to ensure the correct use of information by implementing operating procedures to secure the information that we collect and

information shared with us by our partners. Our security practices are periodically reviewed and enhanced as necessary.

DATA STORAGE POLICIES

All information is stored electronically in files and folders on OPHRDC's Network Shares and Network Drives (not on user's Desktop, C drive or Mobile Device). All Mobile Devices (laptops, cell phones) and User computers must be encrypted using approved encryption techniques and/or password protected. The C Drive and Server drives are encrypted at rest. OPHRDC databases are backed up daily.

All data are stored in Canada. Core data is stored electronically for an indefinite period and is not deleted at specified times. OPHRDC maintains a longitudinal file of all licensed physicians in Ontario that began in 1992. OPHRDC frequently receives requests for long-term analyses. In addition, the historical data serves as a valuable resource for providing historical perspective and validation of more current data. However, specific data (ie. for a one-time study) may be stored electronically for a defined period and may be deleted at a set time. At that point, the specific data will be deleted from both the main server and backup server by BIT, and a certificate of permanent destruction will be provided.

When OPHRDC computers are repurposed (ie. donated due to replacement or dysfunction), all data are first deleted by BIT using industry standard methods. When equipment such as PCs or servers are discarded, all data on the hard drive are destroyed by BIT using industry standard methods. This includes removal and destruction of the drive(s), first by brute force (ie. hammer), then by shredding (completed by BIT's contractor at secure facility).

DATA STORAGE CENTRE

Previously, the server room was located in the office, which required keyed entry at all times. As of 02OCT2018, there is no physical server onsite. We now work directly from our server at the Tier 3 Data Centre hosting facility located in the Greater Toronto Area (GTA), Canada, and operated by Terago Networks located in Mississauga, Ontario. The systems are designed to provide maximum availability of service for power and internet connectivity.

DATA PROTECTION

OPHRDC data is protected by redundant server architecture, backup systems, disaster recovery plans and multiple layers of user authentication.

BIT performs full systems backups on a weekly basis and incremental backups daily. Backup Data is transferred nightly to Backup Data Center located in Vaughan, Ontario. Nightly incremental backups are retained for one (1) week. Weekly backups are retained for four (4) weeks.

Contact Us

Any questions or comments about these practices can be directed to:

Neil Johnston
Director
Ontario Physician Human Resources Data Centre (OPHRDC)
565 Sanatorium Road, Room 209
Hamilton, ON L9C 7N4
Phone (905) 296-4811 ext. 505