

Best Practice Guidelines for Protecting Patient Data during Billing Processes

Individuals who are completing OHIP billing for LHSC or SJHC Physicians:

- Will normally be either:
 - i) employees of the hospital with which the physician or physician group is affiliated, or
 - ii) individuals hired privately by a physician or a physician group and work within LHSC and/or SJHC premises, for whom the physician has:
 - completed a Declaration and Release and
 - documented through Medical Affairs as a private hire, or
 - iii) an external vendor whose business includes Physician billing
 - iv) individuals privately hired by a physician or a physician group and working outside of LHSC and/or SJHC premises
- individuals in group i) and ii) above must complete the affiliated hospital's Privacy and Confidentiality Education Program and submit a Privacy and Confidentiality Agreement to the Privacy Office. The physician is responsible to validate completion by contacting the Privacy Office prior to permitting the individual access to confidential information.
- It is strongly recommended that physicians consider having Individuals in group iii) and iv) sign a similar privacy agreement to protect yourselves should a privacy breach occur.

The Physician or group is ultimately responsible for the actions of individuals they hire to perform billing functions. As per hospital policy, failure to take reasonable steps to secure confidential information may result in disciplinary action, up to and including termination of employment/contract or loss of appointment or affiliation with the organization.

It is strongly recommended, to protect the physician and the organization's patients' information, that physicians have a signed contract with any individual or vendor who the physician is privately hiring to complete billing. Sample wording that needs to be in that contract is appended to these guidelines.

At minimum, it is recommended that the required elements of any contract should include:

- binding the individual to maintain confidentiality of the information, even beyond termination of contract
- that access to identifiable personal health information and information about the physician are provided to the individual solely for the purpose of completing OHIP billing and must not be used by the individual for any other purpose or shared with anyone
- measures the individual must take to secure the information including,
 - physical security measures, including the requirement that identifiable patient information must not be removed from the hospital
 - electronic security measures, including storage identifiable patient information only on hospital network systems and not on portable devices or home computers
 - storage and retention of both hard copy and electronic billing information
 - requirement that the individual adhere to hospital policies related to privacy of security including:
 - Confidentiality
 - Security of Confidential information
- that breach of the terms of contract may be cause for termination of the contract, or other actions deemed appropriate by the hospital and or physician
- contain an indemnification clause

Security of hardcopy and electronic information

Confidential information about patients must comply with the Security of Confidential Information policy:

LHSC: http://appserver.lhsc.on.ca/policy/search_res.php?polid=GEN028&live=1

SJHC: http://intra.sjhc.london.on.ca/policy/search_res.php?polid=GEN003&live=1

In addition to requirements outlined in the policy, measures specific to physician billing include:

- Removal of identifying patient information in hard copy and/or electronic formats is discouraged.

- If information identifying patients (see definition) in any way must be removed from the hospital to complete the billing the information must be protected by:
 - applying encryption to electronic devices
 - ensuring secure transport and storage of the information as per the Security of Confidential Information policy (if using a courier make sure the company is bonded).

Access to LHSC/St Joseph's electronic patient record systems:

The physician is responsible for:

- requesting access to the hospital's EPR systems and billing software for their agent who requires access for the purpose of billing and revoking that access when no longer required as per the policy on Systems Access
- ensure their agent undergoes training on use of the hospital's EPR system to ensure appropriate use

Breach of privacy, confidentiality or security of patient information:

The physician agrees to notify the hospital's Privacy Office promptly if he/she becomes aware of a privacy or security breach relating to the hospital's patient information used by any individual for the purpose of billing.

In the event of a breach of privacy, confidentiality or security, the physician and Privacy Office will work collaboratively to identify the cause of the breach, identify the affected information, assess the consequences of the breach, undertake and implement possible mitigation measures for the breach such as assistance in recovering lost or disclosed information, assist the hospital to meet it's PHIPA obligation to notify impacted individuals and determine appropriate measures to prevent the recurrence of such a breach to meet the Hospitals obligations under PHIPA.

Any and all costs associated with the investigation of a breach caused by the physician, their employees, or their agents will be paid by the physician.

Appendix 1 to Best Practice Guidelines for Protecting Patient Data During Billing Processes

Sample Contract Template for Physicians hiring individuals or vendors to complete billing:

Dr XXXXX agrees to provide identifiable patient information as well as confidential billing information to XXXXX for the sole purpose of XXXXX completing and submitting Dr XXXX's billing information to the Ontario Ministry of Health.

On signing this Agreement, XXXXX confirms that any confidential information, regardless of format, obtained by (XXXXX {or for vendors - by XXXX or any agent of XXXXX }) will be kept confidential and secure. XXXXX must protect confidential information by making reasonable security arrangements against such risks as unauthorized access, use, disclosure, copying, modification or disposal. XXXXX may not disclose the confidential information to any person, other than Dr XXXX or (LHSC/SJHC). XXXXX must not permit access to or use of the information to any other person/s.

XXXXX must comply with the terms of the following hospital policies, a copy of which are appended to this contract:

- Confidentiality
- Security of Confidential Information

(for vendors - On signing this Agreement, XXXXX confirms that it is compliant with requirements of both Ontario and Canadian Privacy laws, in that it will use confidential information strictly for the purpose of billing the Ministry of Health for services performed by Dr XXXXX. XXXXX confirms that it has a program for education of its staff on privacy, confidentiality and security of information, ensures that employees are aware of their privacy and confidentiality obligations and ensures that employees who resign or are terminated return all confidential information belonging to Dr XXXXX.)

(for individuals - prior to access to any confidential information, XXXXX must complete the {LHSC/SJHC} Privacy and Confidentiality Education Program and submit a signed Privacy and Confidentiality Agreement to the (LHSC/SJHC) Privacy Office.

XXXXX agrees to notify Dr XXXXX and the (LHSC/SJHC) Privacy Office promptly if he/she/vendor name becomes aware of a confidentiality or security breach relating to the confidential information and will cooperate in identifying the cause of the breach, investigation into the breach and attempts to recover the lost or disclosed information.

On expiry or termination of this Agreement, or upon request of Dr XXXXX, XXXXX will cease any and all use of the confidential information and will return it to Dr XXXXX, including any copies, or will destroy it in a manner designated by (LHSC/SJHC), with proof of destruction.

This Agreement confirms that LHSC/SJHC is authorized to audit the privacy (vendor - policies and) practices and security measures of XXXXX at the discretion of LHSC/SJHC, and on reasonable notice, to ensure compliance with this Agreement.

IDEMINIFICATION

Each of the parties (“Indemnitor”) shall indemnify and hold harmless the other parties (including its directors, officers, employees, agents and affiliates) (“Indemnitee”) from and against any and all claims, demands, judgments, actions, causes of action, liability, losses. Costs, damages and expenses, including reasonable legal fees and disbursements, brought against or suffered by the Indemnitee as a result of:

- a) a breach by the Indemnitor of any of its obligations under this Agreement;
and/or
- b) the negligence, willful misconduct or other tortuous act or omission of the Indemnitor or any person for whom it responsible at law in the performance of its obligations under this Agreement.

The indemnitee shall provide prompt written notice of any claim that might give rise to such liability and in the case of third party claims, shall cooperate in the non-monetary defense of such claim. The indemnification obligations in this Agreement shall survive the termination or expiration of this Agreement.