Information and Privacy Commissioner of Ontario

Fact Sheet

Number 10
December 2005

Secure Destruction of Personal Information

This fact sheet includes suggested best practices for the destruction of personal information.

Any organization, whether in the public or private sector, should follow responsible, secure procedures for the destruction of records containing personal information,[1] once a decision has been made not to retain or archive this material.[2] In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – it's the law! All three of Ontario's privacy laws – covering provincial and municipal government institutions and health information custodians – as well as federal legislation covering private sector organizations, require that personal information, including personal health information, be disposed of in a secure manner, whether it be in paper or electronic format.[3]

A recent investigation by the Information and Privacy Commissioner of Ontario into how health records ended up strewn on the streets of downtown Toronto determined that documents containing personal health information had not been securely handled or properly disposed of. This resulted in the Commissioner's first Order (HO-001) under the *Personal Health Information Protection Act, 2004 (PHIPA).*[4] This high-profile incident dealing with paper records containing personal health information highlighted the need for secure destruction practices for both paper records and records in other formats.

Below are the recommended best practices for the secure destruction of records containing personal information.

Match the destruction method to the media

The goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Consider not only the "official" files but any duplicate copies of documents made for in-office use (documents could carry "shred after" dates or "do not copy" warnings).

a) **For paper records,** destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed. Since it is technically possible to reconstruct even cross-cut shredded documents, consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place. Consider whether on-site or off-site destruction is more suitable for your organization.

b) For electronic and wireless media such as floppy disks, CDs, USB keys, personal digital assistants (PDAs) and hard drives, destruction means either physically damaging[5] the item (rendering it unusable) and discarding it, or, if re-use within the organization is preferred, it means employing wiping utilities provided by various software companies.[6] Wiping may not, however, irreversibly erase every bit of data on a drive.

Select and engage your service provider with due diligence

If you are engaging an external business to destroy records, be selective. Look for a provider accredited by an industrial trade association, such as the National Association for Information Destruction, or willing to commit to upholding its principles, including undergoing independent audits. Check references, and insist on a signed contract spelling out the terms of the relationship. (Please see the Appendix for suggested contractual clauses.) The contract should:

- set out the responsibility of the service provider for the secure destruction of the records involved;
- specify how the destruction will be accomplished, under what conditions and by whom;
- require that a certificate of destruction be issued upon completion, including the date, time, location, and method of destruction and the signature of the operator (while a certificate itself cannot prove that destruction has actually occurred, its existence, along with the written service contract, documented reference-checking, accreditation, etc., demonstrates that you have taken reasonable steps to ensure secure destruction has taken place);
- include a provision that would allow you to witness the destruction, wherever it occurs, and to visit the service provider's facility;
- state that employees must be trained in and understand the importance of secure destruction of personal information;
- require that if any of the work is subcontracted to a third party, the service provider must notify you ahead of time, and have a written contractual agreement with the third party, consistent with the service provider's obligations to you;
- specify a time within which records collected from you will be destroyed, and require secure storage pending such destruction.

For further information

The following websites may prove useful:

ARMA Canada *www.armacanada.org*;

ARMA International *www.arma.org*;

National Association for Information Destruction Canada *www.naidcanada.org*;

Canadian Health Information Management Association/Canadian College of Health Record Administrators *www.chra.ca*;

Ontario Health Information Management Association (formerly Ontario Health Record Association) *www.ohima.ca*;

American Health Information Management Association *www.ahima.org/about*.

Notes

1. Personal information is a defined term in the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), and personal health information is a defined term in the *Personal Health Information Protection Act, 2004 (PHIPA)*.

2. Records management policies should spell out how long records will be retained based on legal, professional, and archival obligations and the organization's own specific needs, as well as how to keep track of which records have been archived and which have been destroyed. The type of information that organizations track about disposed-of records may vary with the circumstances. Section 6(2) of Regulation 459 under *FIPPA* requires the head of an institution to ensure that the institution's disposal record (the Regulation's term for the tracking instrument) does not contain personal information. See also the IPC's *PHIPA* Fact Sheet #1, *Safeguarding Personal Health Information* (http://ipc.on.ca/docs/fact-01-e.pdf) and the *Physician Privacy Toolkit* and the *Hospital Privacy Toolkit* referred to in that fact sheet for specific information about the disposal of personal health records.

3. *PHIPA* requires health information custodians to protect personal health information in their custody or control and to ensure that records are retained, transferred and disposed of in a secure manner (see sections 12 and 13). Section 2 of Regulation 459 under *FIPPA* permits provincial institutions to dispose of personal information in only one of two ways: either by transferring it to the Archives or by destroying it. If the institution destroys the personal information, then the head of the institution must take all reasonable steps to ensure that it is destroyed in such a way that it cannot be reconstructed or retrieved (see section 5 of the Regulation). Municipal institutions under *MFIPPA* are encouraged to follow the same rules. Private sector organizations in Ontario are subject to the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), including the 10 fair information principles of Schedule 1. For example, clause 4.5.3 of Schedule 1 requires organizations to develop guidelines and implement procedures governing the destruction of personal information, and clause 4.7.5 requires care to be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

4. See Order HO-001, available on the IPC's website at www.ipc.on.ca/docs/ho-001.pdf. Previous privacy complaint reports involving the disposal of personal information include PC-000022-1, PC-010043-1, PC-020014-1, I97-049M and others.

5. Snapping into pieces, hammering, drilling holes into, obliterating or pulverizing have been suggested.

6. If office machines such as photocopiers, fax machines, scanners and printers contain storage devices (such as a hard drive) that have not been disabled, these should be overwritten, or removed and destroyed, when the machines are replaced.

Appendix – Sample Contract Clauses for the Secure Destruction of Records Containing Personal Information*

Please note that these sample contract clauses are **not intended to provide legal advice and must **not** be contstrued as such. It is prudent to consult your own legal counsel prior to entering into any agreement.*

- [Company] agrees that it will destroy the records collected from [Client] in the following manner:
    - [Specify manner of destruction applying to each category of records. Paper records should be destroyed using a method that is at least as secure as cross-cut shredding, or better. Records identified by [Client] as being highly sensitive should be destroyed by pulverizing or incinerating them.]
- [Company] agrees that its services will be performed in a professional manner, in accordance with industry standards and practices, by properly trained employees. [Company's] employees understand that breach of the security and confidentiality of [Client's] information may lead to disciplinary measures.
- If [Company] engages the services of a third party to perform all or part of the services under this contract, [Company] shall notify [Client] ahead of time.
- If [Company] engages the services of a third party to perform all or part of the services under this contract, the third party shall agree, in a written contract with [Company], to comply with all standards and procedures required of [Company] by [Client]. [Client's] records will not be transferred to any third party other than for the purposes of performing record destruction under such a subcontract.
- A copy of the subcontract between [Company] and a third party shall be provided to [Client] at the time it is entered into. [Company] remains liable for all services performed for [Client].
- [Company] shall provide [Client] with a Certificate of Destruction documenting the date, time, location and method of destruction and bearing the signature of the operator, either at the conclusion of the destruction process or, if destruction is performed as part of a regularly scheduled event, at specified regular intervals as agreed to by [Company] and [Client].
- If requested by [Client], an authorized representative of [Client] may, at any time, inspect the record destruction process, including by attending at [Company's] facilities.
- [Company] agrees that any records collected from [Client] for the purpose of destruction will be destroyed within [**] days of collection. Pending their destruction, the records shall be stored in a secure manner, ensuring physical security and restricted access. [Company] will know at all times the location of [Client's] records and will advise [Client] of this location if requested.

Fact Sheet

is published by the **Office of the Information and Privacy Commissioner of Ontario**.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA
M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Cette publication, intitulée « Feuille-info », est également disponible en français.

30% recycled paper