Guide on Handling Documents Used in Peer Review

Application and peer review documents contain personal information as well as information whose unauthorized disclosure could reasonably be expected to cause serious injury (such as prejudicial treatment or loss of reputation or competitive advantage) to an individual, organization or government. As such, these documents are subject to regulation under the *Privacy Act*, the *Access to Information Act* and the Policy on Government Security (PGS). Measures must be followed to ensure that information contained in applications, internal and external reviews and committee discussions remain strictly confidential1. Improper or unauthorized collection, use, disclosure, retention and /or disposal of this information can result in a privacy breach.

Document Handling Procedures

1. Storage

All materials used in the peer review process must be stored in a secure manner to prevent unauthorized access:

- All paper copies of applications and peer review documents must be stored in a locked cabinet. They should never be left unattended in an open area.
- IT media (e.g. CDs, USB keys) containing peer review files must be stored in a locked cabinet.
- When possible, avoid saving local copies of applications and peer review documents. If electronic versions of peer review information are required, please save them on your computer hard drive or IT media, using security measures such as secure passwords on your desktop, laptop and / or at the file level. Never save peer review documents on your organization's network.
- Delete electronic files as soon as you are done with them.

2. Transmission

As information contained in peer review documents is confidential, its transmission should be restricted to times when it is absolutely required:

- All reviews should be posted on ResearchNet and not sent via e-mail.
- Applications and / or peer review documents must be encrypted2 prior to sending by e-mail.
- Paper copies and / or IT media containing peer review files must be sent by 1st class mail, priority, registered mail or by reliable private courier services.

---

1 The use of the term 'Confidential' is strictly to ensure comprehension and is not used in accordance with the Government of Canada Policy on Government Security (PGS) Glossary. The information contained in an application is actually designated as 'Protected B' within the context of the PGS.

2 Protected B information requires the use of an application which offers PKI type encryption, such as Entrust, Tovaris, Verisign PKI, etc.

3. Destruction

When no longer required, peer review related documents and files must be destroyed using a secure method:

- IT media containing peer review documents must be returned to CIHR for destruction.
- Paper copies may be shredded at your institution or may be returned to CIHR for destruction.
- All locally saved electronic documents must be deleted.

Privacy Breach Process

If you suspect that applications or peer reviews documents have been compromised (e.g. stolen laptop, lost USB key, misplaced application document), please inform your peer review coordinator immediately.

For more information, please contact:

Senior Security Operations Officer
Canadian Institutes of Health Research
160 Elgin Street, AL 4809A
Ottawa, Ontario K1A 0W9
Tel 613-948-4636
Fax 613-954-1800
Email: security@cihr-irsc.gc.ca