EDGE CLINICAL RESEARCH MANAGEMENT SYSTEM

PRIVACY BREACH MANAGEMENT PROCEDURES

Privacy is the right of an individual to be left alone, to be free of unwarranted intrusions. It is also the right of an individual to retain control over his or her personal information and to know the uses, disclosures and whereabouts of that information. A **Privacy breach** involves improper or unauthorized creation, collection, use, disclosure, retention or disposal of personal information.

In the event that a privacy breach related to EDGE Clinical Research Management data is discovered by an Alberta Innovates (AI) employee, the following steps will be followed to assess, contain, and report the breach to the appropriate individuals. The steps outlined below are provided as a guide to individuals assessing and reporting a privacy breach stemming from the use and dissemination of information housed in the EDGE Alberta organization by employees of AI.

1. Assessment

1.1. Employees and contractors of AI are expected to report EDGE privacy or information breach to the ACRC manager when it is first discovered.

1.2. The ACRC Manager will identify whether the breach involves employees of AI only or employees of an organization sub-licensing EDGE from AI. In the event the breach involves only employees of another organization, the ACRC Manager will notify the Privacy Officer (PO) of the respective organization and assist the PO with providing any information or facilitate communication between the organization and EDGE UK for breach containment as required.

1.3. In the event of an actual or suspected breach the ACRC Manager will notify the FOIP Coordinator (2019: Jeannie Brochu-who will engage AI's Breach Response Team) and the EDGE UK team (email: edge@soton.ac.uk) as soon as possible after the discovery of a privacy breach. Occasionally, a breach may occur before a long weekend; therefore, it is recommended to notify the FOIP Coordinator via email as soon as possible.

1.4. A privacy breach may also involve a breach of security. In these situations, the ACRC Manager needs to ensure coordination with the Executive Director of IT (2019: Brent Ives). It is important to involve the FOIP Coordinator, and Exec. Director IT to ensure the privacy of individuals and the security of assets are taken into account in the resolution process.

1.5. The ACRC Manager will perform a preliminary assessment to outline how the privacy breach occurred. This assessment can be performed using the **Preliminary Assessment and Containment Tool (Appendix A)**.

1.6. In the event the ACRC Manager has answered yes to the questions contained within the Preliminary Assessment and Containment Tool, the ACRC Manager will take immediate action to contain the breach.

1.7. While containing the breach, the ACRC staff will assist with documenting the circumstances, as extensively as possible, within a short period, that gave rise to the privacy breach, including an inventory of the personal information that has been compromised.

1.8. The ACRC Manager will take immediate action to contain the breach and to secure the affected records, systems, email or websites. For example, immediate action to contain the breach may consist of the following:

1.8.1. Suspend or terminate EDGE user accounts for those accessing exposed information or files.

1.8.2. Remove, move, or segregate exposed information or files, i.e., take all necessary steps to prevent further unauthorized access and disclosure;

1.8.3. Retrieve any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person;

1.8.4. Return the documents to their original location or to the intended recipient;

1.8.5. Advise the employee to cease transmission of email or correspondence to the incorrect address; and

1.8.6. Request the recipient to delete all affected email, correspondence and records.

1.9. In some instances, it may be necessary to shut down access to EDGE Alberta temporarily to permit a complete assessment of the breach and resolve vulnerabilities. Additional considerations may be revoking access, modifying passwords or correcting weaknesses in physical security. This will be undertaken in consultation with the EDGE-UK team and AI Exec. Director, IT (Brent Ives).

2. Report

2.1. Following the discovery and containment of a privacy breach, an assessment will be developed by the required individuals to determine the level of the breach assessment required. Completing the assessment will require the identification of the following:

2.1.1. Individual(s) who may have caused the breach;

2.1.2. Potential witnesses who may have information related to the breach;

2.1.3. Affected parties whose personal information was disclosed, accessed, stolen or lost; and

2.1.4. The institutional sector (public or private) or third party that is responsible for the personal information involved (external stakeholders).

2.2. Upon submission of the assessment to the FOIP Coordinator, and/or the AI Exec. Director IT (Brent Ives), an investigator will be assigned to assist in documenting the privacy breach and provide support and guidance to the ACRC Manager including generating a full report including;

2.2.1. Details on the circumstances that gave rise to the breach: what happened, where it happened, when it happened, and how it was discovered;

2.2.2. Inventory of the personal information that was compromised;

2.2.3. Identification of the parties or persons whose personal information has been wrongfully disclosed, accessed, stolen, compromised or lost;

2.2.4. Identification of the institutional sector or third party responsible for the personal information involved; and

2.2.5. All other relevant information (e.g., previously similar or related privacy breaches).

2.2.6. The risk impact of the breach with consideration as to the personal information involved, the cause and extent of the breach, individuals affected, the source of the breach, and foreseeable harm from the breach.

3. Notification

3.1. If a privacy breach creates a risk of harm to the individual, those affected will be notified. Prompt notification of individuals in these cases can help them mitigate the damage by taking steps to protect themselves.

3.2. The FOIP coordinator may notify relevant authorities (i.e. OIPC) using the report form in **Appendix B** of the privacy breach at this stage of the process if not already done.

3.3. For internal notification: the FOIP Coordinator may determine the extent of the notification required to notify AI's CEO, Senior Management, Human Resources, Legal Services and Communications, as required.

3.4. The Privacy Breach report generated in Step 2.2 can be modified and anonymized to notify relevant staff within AI of the privacy breach.

3.5. The ACRC Manager will assist the FOIP Coordinator, and other relevant senior management in the development of notification letters to affected individuals as well as external stakeholders.

3.6. The FOIP Coordinator is the single liaison for AI, the ACRC, and EDGE Alberta when notifying the OIPC.

4. Prevention and Mitigation Strategies

4.1. Once the breach has been resolved, the ACRC and EDGE Alberta staff will meet with the AI Breach Response Team to develop a plan to review the breach, identify a plan and implementation strategy to prevent the breach from occurring again and mitigate any other identified risks arising from the breach.

Appendix A:

ACRC (EDGE-ALBERTA) Preliminary Assessment and Containment Tool

If the answer is **yes** to any of the following questions, contact the Privacy Officer, the FOIP Coordinator, and as required the Director, IT. Be sure to:

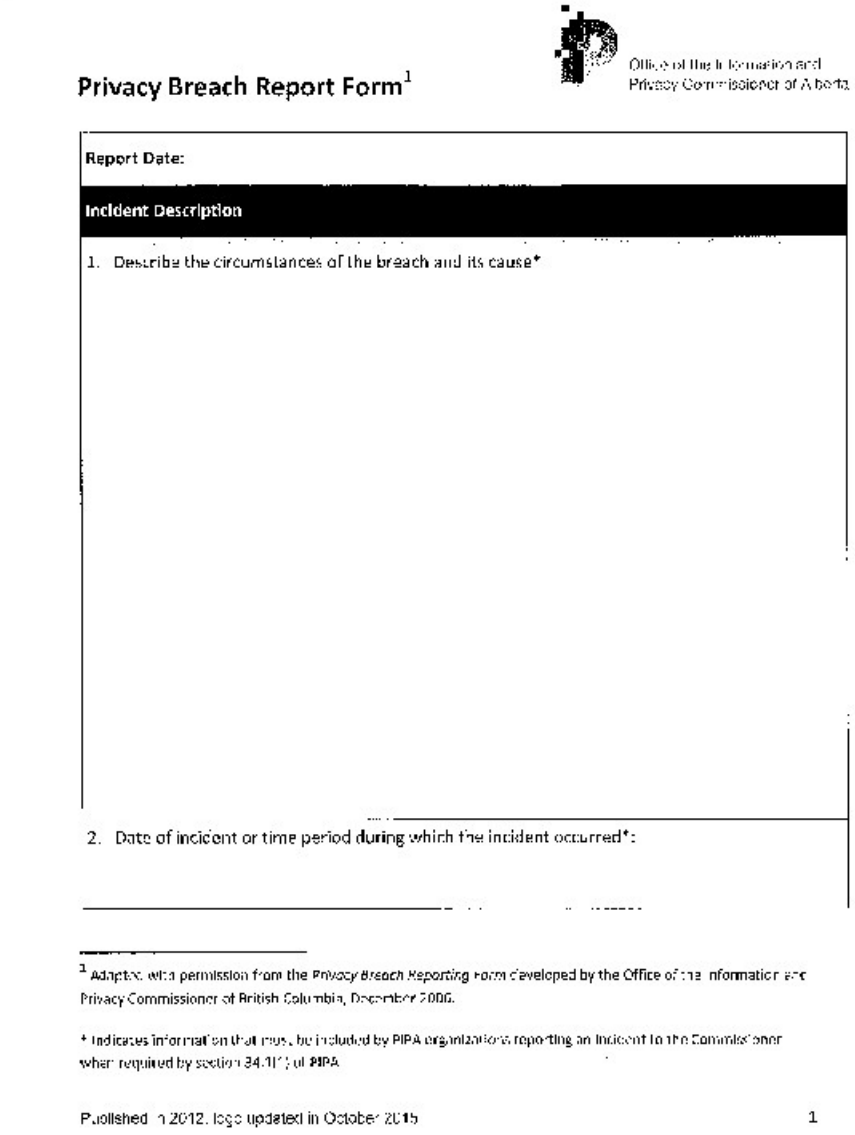
a) Establish which parties need to be made aware of the breach (such as unintended recipients of personal information) and inform them of what they are expected to do to assist in the containment exercise.
b) Establish whether there is anything you can do to contain the breach, recover any losses and limit the damage that the breach can cause.
c) Complete a ***Preliminary Report***, i.e., document all activities that relate to the breach, including how the incident was contained. Include a date and time log, as appropriate, such as who did what and when.

Preliminary Assessment	Yes/No	Suggested Containment Strategies
1. Was there an abuse of access privileges (e.g., unauthorized access or use of records that contain personal information)?		a) Immediately restrict, suspend or revoke access privileges until completion of the investigation. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Attempt to retrieve the documents in question, and document the steps taken. **d) Contact the Access to Information and Privacy officials and the Chief Privacy Officer if required.** e) Complete a *Preliminary Report*.
2. Was personal information inappropriately disclosed (e.g., improper application of severances (material removed or blacked out), incomplete de-identification)?		a) Attempt to retrieve documents. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. **d) Contact the Access to Information and Privacy officials and the Chief Privacy Officer if required.** e) Complete a *Preliminary Report*.
3. Was personal information lost (e.g., through the mail, during a move or on a misplaced electronic device)?		a) Attempt to retrace steps and find the lost document(s). b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Conduct an inventory of the personal information that was or may have been compromised. **e) Contact the Access to Information and Privacy officials and the Chief Privacy Officer if required.** f) Complete a *Preliminary Report*.

1

Appendix B.

https://www.oipc.ab.ca/resources/breach-report-form.aspx



Privacy Breach Report Form[1]

Office of the Information and Privacy Commissioner of Alberta

Report Date:
Incident Description
1. Describe the circumstances of the breach and its cause*
2. Date of incident or time period during which the incident occurred*:

[1] Adapted with permission from the *Privacy Breach Reporting Form* developed by the Office of the Information and Privacy Commissioner of British Columbia, December 2006.

* Indicates information that must be included by PIPA organizations reporting an incident to the Commissioner when required by section 34.1(1) of PIPA.

Published in 2012. Logo updated in October 2015 1