**Appendix A: Provincial Reportable Incident Response Process Form**

This form is used to engage the Provincial Reportable Incident Response Process (PRIRP). The form is to be updated and submitted as the appropriate information is gathered concerning the incident for each of the five phases of PRIRP. Do not include health information or sensitive information when completing this form. Submit completed form to [AH.Security@gov.ab.ca](mailto:AH.Security@gov.ab.ca).

If you have any questions call the *EHR Helpdesk at* **1.877.931.1638or 780.412.6778**or contact the Alberta Health Security Team at **780.643.9343**.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Phase 1 Incident Detection and Reporting**  *Reporting stakeholders with a reasonable suspicion of a real or potential threat to health information are to complete and submit Phase 1 of the form. Breaches of health information should also refer to HIA Breach Reporting requirements identified on page 3 of PRIRP.* | | | | | |
| **Reporting Stakeholder Details ­/ Identify and Report (PRIRP 1.1)** | | | | | |
| Date of Incident: |  |  | Phone Number: | Click or tap here to enter text. |  |
| Full Name: | Click or tap here to enter text. |  | Email Address: | Click or tap here to enter text. |  |
| Organization: | Click or tap here to enter text. |  | | | |
| Job Title: | Click or tap here to enter text. |  | | | |
|  | | | | | |
| **Incident Information** | | | | | |
| Include description of threat (what type of health information has been disclosed, accessed inappropriately, lost or stolen, estimates on number of records or individuals impacts, when the threat was discovered, how long the threat has existed, and any other relevant details. | | | | | |
| It was discovered that access to the Health Economics Unit (HEU) mount point on server iedm2a16 was open to Russell Timmerman who is not a member of the mpheu control group. The mpheu control group membership is meant to lmit the people who can access the HEU mount point to the people whom are members of the control group. Further investigation has shown that the control group for the HEU mount point is sassrusr a group with a much larger membership pool that includes all BIE users. | | | | |  |
|  | | | | | |

|  |  |
| --- | --- |
| **Phase 2 Classification and Support**  *Complete and submit as directed by PRIRP Incident Response Team (IRT) Lead with updated information gathered from incident source.* | |
| **Review and Confirm Details (PRIRP 2.1)** | |
| Confirm incident details and include any updated information from the source of the incident. Include details information on any containment steps taken. | |
| AH Security (Sep 25):  HEU mount point is open to the entire BIE user group (330 users), while only a subset of 14 users of the Health Economics Unit (HEU) should have access. The mount point is used by the HEU as a work area to store analytical data and not considered a source of truth. The data in the mount point may contain individually identifiable health information and is considered Protected B. Access to the group is approved by Nirosha Gunasekara – Senior Data Analyst, Health Economics & Funding. Access to the HEU mount-point is gained through the SAS application or by terminal connection. The mount-point cannot be accessed directly over the internet. Access to external users are available through the GoA Citrix environment which requires multifactor authentication (FOBS). The mount-point is not directly accessible from the internet.  There is documentation of a ticket made 2014 instructing IBM to set the control group for the heu mount point to be mpheu. It is unknown precisely why or how the control group was changed from mpheu to sassusr. A ticket has been opened to have the control group for HEU returned to mpheu. ( IBM TKT: 19267-05) Awating confirmation from program area/BIE that the IBM change has been implemented and tested. |  |
|  | |

|  |  |
| --- | --- |
| **Phase 3 Investigation and Diagnosis**  *Complete and submit as directed by PRIRP IRT Lead with information gathered from technical and operational sources.* | |
| **Analysis and Diagnosis Update (PRIRP 3.1)** | |
| Include technical and operational analysis and diagnostic updates from any parallel incident owner investigation, what is known about cause of the incident, and any identified impacts to health or other confidential information. | |
| There is documentation of a ticket made 2014 instructing IBM to set the control group for the heu mount point to be mpheu. It is unknown precisely why or how the control group was changed from mpheu to sassusr. A ticket has been opened to have the control group for HEU returned to mpheu. ( IBM TKT: 19267-05) |  |
|  | |

|  |  |
| --- | --- |
| **Phase 4 Resolution and Recovery**  *Complete and submit as directed by PRIRP IRT Lead with information gathered from resolution activities.* | |
| **Implementation and Monitoring Update (PRIRP 4.1)** | |
| Include updates regarding resolution plan, testing of resolution, and system monitoring results. | |
| Awating confirmation from program area/BIE that the IBM change has been implemented and tested. |  |
|  | |

|  |  |
| --- | --- |
| **Phase 5 Incident Review and Closure**  *PRIRP IRT Lead completes with information gathered from resolution activities; used to make recommendations to involved parties.* | |
| **Incident Review (PRIRP 5.1)** | |
| Review details provided in above phases to identify policy, process, procedures, or measures needing to be implemented or changed. | |
|  |  |
| To reduce risk of unauthorized access/disclosure of data in mount-points the BIE team is advised to;  \* Maintain a complete list of all mount-points, associated user groups and data classification.  \* Periodically review and confirm membership of each user groups  \* Clean up transitory data  \* Periodically review and confirm entire BIE user membership  ITO is advised to work with BIE to enable logging of user activity such as create, read, update, delete. | |