**Reporting and Investigating Privacy Breaches and Complaints:**
**Fact-finding Interview Guide**

*This tool may be used for the fact-finding interview and customized to be applicable to the circumstances. The questions are not all inclusive and other questions should be considered in consultation with human resources and/or the manager or supervisor*.

| | | | | | |
|---|---|---|---|---|---|
| Incident No. | | Occurrence No. | | Complaint No. | |
| Date of Interview: | | | | | |
| Interviewee: | | | Interviewer(s): | | |
| | | | | | |

Where an audit of a patient-centric or user-centric report of activity within an electronic health record system has identified questionable activity, it is important to inquire about the user's reasons for accessing the information. The user's response will help to inform decision making and determine whether a real risk of significant harm exists for individual(s) whose information was accessed.

The purpose(s) for access, as explained by the user, should be validated with corroborative information such as scheduled appointments, paper records, staff schedules, responsibility of staff role, etc.

**Note:** Maintain appropriate documentation about the interview.

**QUESTIONS:**

| | |
|---|---|
| **1.** | **Why did you access the personal health information? OR**<br>**Why did you access the personal health information belonging to: ?** |
| | An authorized purpose. |
| | → Users should only be accessing information for an authorized purpose such as the provision of health care or to carry out the responsibilities of their role. Access must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed. |
| | Consent from family/friend/co-worker. |
| | → An individual cannot give a user consent to breach the legislation or organizational policy (i.e. looking up information for a family/friend/co-worker). |
| | Denies Accessing the information. |
| | → The report is documented evidence of the user's activity and is treated as factually correct, regardless of whether a user recalls having accessed a record or not.<br>→ Users are required to log out of an electronic health record system and/or the network when they leave their workstation. Stepping away without logging out is an unacceptable rationale.<br>→ If the user denies having done something that is represented on the privacy audit, they are to be reminded that they are accountable for any activity under their user name. |
| **Notes:** | |

| 2. | **What did you do with the information?** |
|---|---|
| | Print or take copies? |
| | Share the information with anyone? |
| | → This includes verbally sharing the information and includes sharing within the organization or with others outside the organization (i.e. at home). |
| | Other? |
| *These are important details to be aware of when assessing the risk to the affected individual(s) and critical information to have available when notifying individuals that their information has been breached. If reassurance can be provided that the information was not retained or shared it is often a comfort.* | |
| **Notes:** | |

| 3. | **Is there anything else you wish to tell us about your use of the system?** |
|---|---|
| | No. |
| | Yes. |
| →All activity leaves an auditable record in electronic health record systems. | |
| **Notes:** | |

| 4. | **What is your understanding of *The Personal Health Information Act* (PHIA) and our obligations, as trustees, under the Act?** |
|---|---|
| **Notes:** | |

A trustee's obligation is to take all practicable steps to prevent breaches from occurring and to understand the extend and the scope of any breach. If new information comes to your attention, you may need to investigate it. Candid conversations during an interview may bring to light other activities not captured during the audit of the user's activity in the electronic health record system. As you receive new information, you are obligated to investigate as well.