Capital Health

Privacy Breach Protocol Guidelines

1. **Identify the Breach:** Date, time, location, length, type and extent of breach need to be established to contain the breach.

2. **Immediate Remedial Action**:
   - Were hard copies of any faxed personal information retrieved or was there confirmation that the recipient(s) securely disposed of the fax?
   - Was the unopened GroupWise email recalled or was the GroupWise recipient(s) who had opened the email contacted to request the email be deleted and hard copies securely destroyed?
   - Regarding a recipient(s) not on the GroupWise system, did you contact the recipient(s) to request deletion of the email and secure disposal of any hard copies?
   - Will the breach allow access to any other personal information, and if so, were steps taken to avoid this potential additional breach?
   - If an electronic device and paper records containing personal information was stolen, did you immediately contact security (if within Capital Health) or the police (if outside Capital Health)?

3. **Internal Notification:** Notify your supervisor and the Privacy Officer.
   - If the breach involves a website, the ITS Director will be contacted
   - If the breach is serious or could be potentially serious, Legal Counsel needs to be contacted.
   - If the breach is or will be a matter of public interest, the Media Advisor.

4. **Investigation and Documentation:**
   - Were the immediate remedial actions effective?
   - Is there enough documented evidence about the incident to determine the series of events that lead to the breach?

5. **External Notification:** After the Privacy Officer consults with Legal Counsel, one or more of the following may need to be notified:

   - Individual(s) whose privacy has been breached;
   - The Nova Scotia FOIPOP Review Officer;
   - Communications at the Department of Health & Wellness (through CH Media Advisor);
   - Other individuals who may have been affected by the breach.

6. **Follow-up and Long Term Remedial Action:**
   - Was the privacy breach protocol followed?
   - Do new or amended policies, procedures and/or training required to prevent reoccurrence of the breach?
   - What plans have to be developed to lessen the likelihood or eliminate the possibility of another breach?

For further information or assistance, please contact:

Capital Health
Privacy Officer 473-4866
Posted: May 19, 2011