



## **KBRH Health Foundation**

---

1200 Hospital Bench  
Trail, BC V1R 4M1  
250.364.3424 Fax: 250.364.5138  
www.kbrhhealthfoundation.ca  
facebook: kbrhhealthfoundation.ca

### **Policies & Procedures**

#### **3.0 Information Management**

##### **3.1 Privacy Protection (Adopted 09-19-16)**

###### **Policy:**

The Foundation will abide by the principles of and remain compliant with all applicable provincial and federal laws when collecting, retaining, and revising information.

###### **Purpose:**

To ascertain required personal and organizational information to adequately support the mission of the Foundation, while ensuring the integrity of the Foundation by respecting privacy and access to information. To ensure appropriate collection, management, maintenance, preservation and disposal of records and information.

###### **Procedure:**

- a. Maintain and adhere to the Donor Bill of Rights.
- b. The Chair must appoint a Director as Privacy Officer who will be the liaison for any person having any personal information on file with the Foundation.
- c. Introduce any person or organization to the Privacy Officer if that person or organization requires a liaison with the Foundation on a privacy matter.
- d. If a privacy matter occurs or a potential breach is reported, Foundation staff and the Privacy Officer shall refer to and utilize the KBRH Health Foundation's Privacy Policy: Procedure, Reporting and Compliance documents to investigate the incident.
- e. Any release of information requests should follow procedures outlined in the KBRH Health Foundation Privacy Policy: Procedure, Reporting and Compliance document.
- f. Verification of a donor's identity must occur prior to any release of information from a donor's personal account.
- g. Requests made by a donor, for personal information to be released to a third party, must occur by written request only and be authorized through completion of the KBRH Health Foundation Privacy Policy: Authorization to Release Information form.
- h. Any third party requesting information from a donor's account, must

prove their legal authority. Written evidence that the requester is a personal representative of the donor must be provided and completion of the KBRH Health Foundation Privacy Policy: Third Party Authorization to Release Information form must occur.

- i. Responses to written requests for personal information should occur within 30 days, and in writing.
- j. Ascertain and record only necessary information.
- k. Use information only for the purpose for which it was ascertained, and do not disclose information by way of sharing, renting or selling it to a third party.
- l. Develop an electronic database, supported by hard copy files when appropriate, on current and potential donors and Foundation members.
- m. Maintain the integrity of the information by making revisions on a timely basis, including the notation of those who wish not to be contacted.
- n. Delete or destroy unneeded electronic or hard copy information at least once a year.
- o. Personal information collected must be retained for one year, after which it must be destroyed, if the purposes of collection are no longer served and there is no legal or business purposes for keeping it.
- p. May delete or destroy a donor's information file after a minimum seven years of inactivity, keeping only the donor's name, last known address, and total donation revenue, donors of endowed gifts and estates excepted.
- q. Secure the information in the offices of the Foundation and in controlled access computer data storage.
- r. Backup electronic database daily, including all pertinent financial information.
- s. The Director of Development is responsible for informing the Privacy Officer, Executive and the Board of any privacy legislation or regulation relevant to the Foundation.

## **KBRH Health Foundation Privacy Policy: Procedure, Reporting and Compliance**

### **Challenging Compliance**

Individuals have the right to challenge an organization's compliance with applicable privacy legislation. If this occurs, staff are directed to provide a report which addresses the concerns and includes: the KBRH Health Foundation's privacy policy, a synopsis of protocol followed to maintain privacy, and a remediation plan for any omitted/noncompliant/unaddressed practices. This report will be signed off on by the Privacy Officer and provided to the complainant.

### **Reporting on Overall Privacy Policy and Compliance Activities**

Foundation staff will review the Privacy Policy in the first quarter of each year. Annually, within the first quarter of the year, the DOD will present a compliance report to the Privacy Officer(s), Executive and Board, encompassing all aspects of the KBRH Health Foundation's Privacy Policy. Adjustments will be made as necessary, with approval of the Executive and Board.

### **Risk Assessment & Privacy Audit Check List**

Risk Assessments will be conducted on an annual basis, using the following check list, to ensure compliance with applicable legislation.

1. Privacy Officer Appointment
2. Collection, Use and Disclosure of Personal Information
  - a. Must inform individuals of reason and obtain consent for collection, use and disclosure of personal information
  - b. Personal information collected, used or disclosed for appropriate purposes and limited to those purposes
  - c. Act with openness, accountability and transparency at all times.
3. Access to and Correction/Annotation of Personal Information
  - a. Maintain accurate records
  - b. Individuals have a right to access and correct/annotate only their own personal information
  - c. Requests for personal information received directly from an individual donor pertaining to his/her donor account can occur upon verification of the donor's identity. Verification of identity can occur by confirming donor information through the use of a minimum of 2 questions such as: mailing address, spouse's name, last donation made, designation of last donation, or ideally showing identification such as a driver's license, if the donor presents in the office in person.

- d. Requests made by a donor, for personal information to be released to a third party, must occur by written request only and be authorized through completion of the KBRH Health Foundation Privacy Policy: Authorization to Release Information form.
  - e. Any third party who is requesting information from a donor's account, must prove their legal authority. Proof of legal authority must be provided via written evidence that the requester is a personal representative of the donor. Legal authority may include: power of attorney, appointee by court (committee), executor or administrator.
  - f. Third parties shown to have legal authority are required to complete the KBRH Health Foundation Privacy Policy: Third Party Authorization to Release Information form prior to release of any information.
  - g. Surviving spouses, who share a joint account with their partner, do not need to complete an Authorization to Release Information form.
  - h. Response to requests for personal information should occur within 30 days, and in writing.
4. Retention and Disposal of Personal Information
- a. Destroy information (electronic and hard copy) when no longer needed for a specific legal/business purpose
  - b. Annual review and disposal of records
  - c. Maximum retention of records 1 year unless for a specific legal/business purpose
  - d. Secure disposal by shredding or secure shredding bins
5. Security and Access Controls
- a. External office doors locked when office unoccupied
  - b. Safe locked nightly
  - c. Filing cabinets locked nightly
  - d. All blank cheques secured in locked filing cabinets
  - e. Computer system access encrypted using User ID's and passwords
  - f. Computers logged off nightly
  - g. Computer backup- as per IHA protocol
  - h. "Need to Know Policy": Employees have access to the minimum amount of personal information needed to perform duties within the organization, as per their Job Descriptions and Roles
6. Training
- a. All new employees must receive privacy training and education prior to accessing personal information
  - b. Privacy training updates will be provided as required and upon receipt of new information
  - c. All staff and board members must sign the KBRH Health Foundation: Oath of Office, Confidentiality Statement and Statement of Commitment annually
  - d. All volunteers must sign the KBRH Health Foundation: Confidentiality Statement prior to engaging in any Foundation volunteer activities.

## **Procedure In the Event of a Complaint or Privacy Breach**

1. Foundation staff to identify breach/potential breach and/or to receive complaint.
2. Collect all necessary information using the Breach Report Form.
3. Assure complainant that issue will be addressed and outline timeframe in which they can expect to receive return communication.
4. Inform Foundation Privacy Officer of breach/potential breach and/or complaint.
5. Privacy Officer to speak to Foundation staff to record their information about the event.
6. Privacy Officer to speak to complainant if required.
7. Assess if situation is a breach of privacy or legitimate complaint, considering the scope of the issue.
8. Recover information as soon as possible and to the fullest extent possible, maintaining records of requests.
9. Assess why breach occurred: ie; mistake, misunderstanding, carelessness, intentional, other.
10. Contact complainant with respect to resolution and remediation and discuss what is required.
11. Implement steps to prevent future breaches/complaints. ie; training, policy change, revise security, etc.

## **Assessment Criteria for Privacy Breach**

Breach Report Form should be completed to assess and identify each privacy breach.

### **1. Incident description: Identify:**

- Identify the incident.
- Date of the incident?
- When the incident was discovered?
- How was the incident it discovered?
- Location of the incident?
- Cause of the incident?

### **2. Breach containment and preliminary assessment:**

- Immediately contain the breach and recover information if possible.
- Designate an appropriate individual to lead the initial investigation.
- Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance.
- If the breach appears to involve theft or other criminal activity, notify the police.
- Do not compromise the ability to investigate the breach. Do not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

### **3. Evaluate the risks associated with the breach. Determine:**

- What personal information was involved
- What the cause and extent of the breach was

- How many individuals have been affected and who they are
- What harm could result from the breach
- Identify physical security in place at time of incident
- Identify technical security in place at time of incident
- Assess type of harm(s) and level of harm that may result
- Assess likelihood of harm occurring

**4. Notification:**

- Determine whether affected individuals should be notified
- If they are to be notified, determine when and how, and who will notify them
- Decide what should be included in the notification
- Determine if others should be informed (i.e. privacy commissioners, police)
- Describe steps taken to notify individuals

**5. Prevent future breaches**

- Describe steps taken to reduce the risk of harm to individuals
- Implement appropriate measures to prevent future breaches

**KBRH Health Foundation Privacy Policy: Authorization to Release Information**

I, \_\_\_\_\_, hereby authorize the KBRH Health Foundation to release the following information to \_\_\_\_\_, from the records pertaining to my donor account.

The information to be released is described or listed as:

The records are required for the specific purpose of:

I understand that my authorization will remain effective from the date of my signature until \_\_\_\_\_, and that the information will be handled confidentially in compliance with all applicable provincial and federal laws.

I understand that I may revoke authorization at any time by written, dated communication.

I confirm that \_\_\_\_\_ has explained the purpose of this form to me and I understand its content. My signature below indicates my consent.

**Requester:**

Signature: \_\_\_\_\_  
Address: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date: \_\_\_\_\_  
Phone #: \_\_\_\_\_

**Foundation Staff:**

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Identification Checked of Requester: Y/N (please circle)

Photocopy of Identification of Requester: Y/N (please circle)

**KBRH Health Foundation Privacy Policy: Third Party Authorization to Release Information**

I, \_\_\_\_\_, in my capacity as \_\_\_\_\_  
hereby authorize the KBRH Health Foundation to release the following information to  
\_\_\_\_\_, from the records pertaining to  
\_\_\_\_\_ donor account.

The information to be released is described or listed as:

The records are required for the specific purpose of:

I understand that my authorization will remain effective from the date of my signature until  
\_\_\_\_\_, and that the information will be handled confidentially in compliance with all  
applicable provincial and federal laws.

I understand that I may revoke authorization at any time by written, dated communication.

I confirm that \_\_\_\_\_ has explained the purpose of this form to me and I  
understand its content. My signature below indicates my consent.

**Requester:**

Signature: \_\_\_\_\_  
Address: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date: \_\_\_\_\_  
Phone #: \_\_\_\_\_

**Foundation Staff:**

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Identification Checked of Requester: Y/N (please circle)  
Photocopy of Identification of Requester: Y/N (please circle)  
Photocopy of Designation of Authority Document: Y/N (please circle)