Privacy review's primary goal is to ensure that the initiatives do not pose a risk to the privacy rights of research participants and that the initiative complies with the applicable privacy legislation.

1. General considerations:

The assessment of whether information is identifiable is made in the context of the specific research.

- **Personal Information:** any recorded information about an identifiable individual, other than contact information.
- **Personally identifiable information (PII)**: information that can be used alone or combined with other sources to uniquely identify, contact, or locate a person. For example, name, IP address, voice, accent, personal opinions, comments, evaluations, individual's educational, financial, criminal or employment status or history, health information.
- **Personal health information (PHI):** identifying information about an individual in oral or recorded form, if the information relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family.
- **Indirectly identifying information:** information that, while not directly identifying, when used or considered in combination with other information, could reasonably be expected to identify an individual.
- Data with unique assigned code is still considered identifiable if the holder of the information also has the master list or key linking codes to individuals.
- Identifiability is dependent on the unique characteristics of information, the amount of information held that may be combined resulting in identification, and on the skills and technology of the data holder that may allow such combinations.

Limit the amount and type of personal information collected.

- The researchers should aim to limit the amount and type of personal information collected. If collection of a personal information is essential to carry out a research project, the researchers are expected to specify the type, amount, and source of personal information and provide reasonable justification for its collection.
    - Limit contact information collected to one or two methods.
    - Use age instead of DOB.
    - Use MRN instead of PHN.
    - Use first three digits of a postal code instead of six.
    - Use month and year instead of full dates.

Research file storage, sharing, and transfer

- All research data must be stored and retained following appropriate physical and digital safeguards and as required per the approved REB application.
- It is recommended that physical files and digital devices are stored in a locked cabinet and locked room with a limited access when not in use; transfer/ upload the files from the portable digital devices to an approved digital storage platform promptly after the recording using a secure connection.
- It is recommended all digital files be stored in encrypted/password protected folders on the PHC's network (VCH, PHSA, and UBC networks are acceptable as well).
- Consider using approved cloud-storage platforms, such as UBC OneDrive, for your research data. Contact PHC IAPO to discuss other cloud-storage options in advance of submitting your REB RISe application.
- Email (even encrypted) should not be used for transmitting sensitive data sets, such as research data sets. Use secure and approved digital file transfer methods, such as IMITS Secure File Transfer Services

(http://imitsinfocentre.healthbc.org/secure-computing/sharing-and-storing-information) or UBC Approved Tools, such as UBC OneDrive (https://it.ubc.ca/services/web-servers-storage/microsoft-onedrive/microsoft-onedrive-faqs).

- Use of external storage devices for storing research data sets is subject to review and approval. Please ensure that IMITS security and encryption guidelines are followed. (http://imitsinfocentre.healthbc.org/resources/how-do-i/security-and-access).
- Use of personal mobile devices to record and/or capture participant study data is not permitted.
- Ensure that you manage the data according to the processes outlined in the approved RISe application. Contact PHC IAPO if you plan to change or expand the use of electronic platform (ex. Do not move a crosswalk file or de-identified research data set to a cloud-storage platform from a PHC network before consulting with PHC IAPO and receiving an approval for PAA on RISe).

Use of clinical systems

- Please be transparent and clear about which clinical systems you are planning to access and the exact data points to be extracted/ transcribed from each system in your RISe application.
- The use of institutional clinical systems (ex. CST Cerner) requires operational approval from the designated department staff (ex. PCM), not the Physician Department Head.
- The access to Cerner is managed by the CST Cerner Access & Provisioning Team. To request access: https://surveys.vch.ca/Survey.aspx?s=89d0c6eb750c45e19f29aff53f04925d
- The use of CareConnect is approved for providing or supporting direct patient care only; any secondary use, such as research or surveillance, has not been approved by the Ministry.
- Clinical data requested from provincial or organizational systems and registries (ex. PharmaNet, PopDataBC) may require additional approvals and information sharing plans. Please contact PHC IAPO with the details of your project first before submitting your REB RISe application.

Data Management and Systems Used

- Ensure that the documents you submit with your application match the processes outlined in the RISe application. One of the most common queries from PHC IAPO to researchers relate to the inconsistencies between the data elements listed in the Case Report Forms (CRFs), Data Management Plan (DMP), protocol, Informed Consent Form (ICF) and what's outlined in the RISe application.
- Develop a comprehensive **Data Management Plan**, including the details surrounding the entire data lifecycle. See https://researchdata.library.ubc.ca/plan/ for further information and DMP templates.
- If your project involves multiple methods and electronic systems (ex. **eConsent, Electronic Data Capture (EDC) systems, wearables, electronic diaries, digital files/ media files**, etc.) include details about each of the systems (including paper-based), including
    - Outline data elements collected by each system (provided as sample CRFs);
    - Where will the data be stored (physical locations of servers),
    - Specify if data is to be stored/ accessed outside of Canada,
    - Who will have access to the data and how will the user access be monitored and managed,
    - How and when will the data be archived and decommissioned,
    - Data transfer methods "when, who, how".
- In general, and applicable to all systems, each user must have their own unique system user account and log in. Sharing of user accounts is not permitted.
- **Crosswalk/ master list** containing key or linking participants' personal information to study codes must be restricted to a limited number of personnel on a "need to know" basis and users no longer requiring access must be promptly removed. The file must be encrypted/ password-protected and be stored separately from the rest of the study data.

- For research projects employing **provisioned devices or commercially available applications** for data capture by the participant, include the following details:
    - Ensure to submit all participant-facing instructions for the technology use with your REB RISe application.
    - Does the technology collect PHI, PII (including IP address), or sensitive information?
    - What type of encryption and authentication methods are used by the technology?
    - Where are the servers located? Where is the helpdesk located?
    - Who will have access to the data collected/ transmitted by this technology?
    - Does the technology use a mobile device management software (is the remote locking and/or removal of data stored on the device possible)?
    - If the technology is being delivered directly to participants who will be responsible for shipping?
- It is recommended to use **REDCap platforms** managed by UBC for your research projects. For more information go to https://redcap.ubc.ca/
- If your project is using an **EDC provided by the Sponsor/ academic collaborator**, please provide sufficient details to facilitate a review as per above.
- If your REB application indicates you will only input month and year, but the EDC tool requires day/month/year, please acknowledge this discrepancy in your application. It is also recommended that this is reflected in the CRF completion guidelines for your site and/ or a site-specific SOP.

Privacy Review and Privacy Impact Assessments

- A Privacy Impact Assessment (PIA) must be completed before implementing or making modifications to the already approved system that involves collection, use, disclosure or storage of Personal Information.
- Contact PHC IAPO for a consultation before submitting your research application on RISe.
- Ensure that all compliance gaps are addressed and reflect the recommendations provided during the consultation process in your data management processes and on the RISe application.

Informed Consent Considerations

- Please **be transparent and provide sufficient information about the systems used** in your project and the geographical locations participants' data will be stored at.
- If **secondary use of anonymized data** sets is planned, ensure that the requirement for data anonymization is reflected in the legal agreement with the Sponsor/ academic collaborator first. Anonymization of data is a very specific technical process that involves multiple steps
- Include **risks associated with emailing**, if applicable: "Personal information that you send in email could be at risk if an email account is compromised. It is your responsibility to protect your accounts from inappropriate access".
- Include **risks associated with using Wi-Fi**, if participants are expected to be using electronic systems: "There are risks associated with accessing and sending information via public and/or unsecured Wi-Fi networks. The information could be viewed and accessed by other users on the network. It is your responsibility to ensure that you use a secure internet connection".
- If the project involves **direct shipment of technology devices to participants**, informed consent should explain that shipments will be made to participants' personal addresses and how will such information be managed.
- If you are planning on using **eConsent platforms**, consider using UBC FoM REDCap. If using a 3rd party platform, a Privacy Impact Assessment may be required. Ensure to include the following details:
    - Where will the electronic records be stored?
    - Will any vendor or 3rd parties have access to the records?

- Is the access restricted to appropriate personnel and how is the user access monitored and managed?
- Is there an audit trail?
- Does archiving retrieve all versions and is appropriately restricted?

2. Recruitment

Use of records (clinical and research)

- Accessing clinical and research records for the purposes of contacting a person requires careful considerations of consent and permissions to disclose such information, as per applicable privacy legislation. Please consult with PHC IAPO if you are planning to use existing clinical or research databases for the purposes of recruitment.
- Please ensure you have appropriate approvals (ex. Regulatory, legal, REB, operational, institutional) prior to accessing clinical records for the purposes of recruitment.
- All personnel accessing the records must adhere to the purposes and processes outlined in the appropriate approvals and sign PHC Confidentiality Undertaking for Researchers.
- Please ensure that you are not accessing or viewing records (clinical or research) of patients/ participants that do not wish to be contacted for research purposes/ did not consent to be contacted for future research. Describe safeguards in place to satisfy this requirement.
- If a patient/ past participant states that they do not wish to be contacted for the purposes of research, promptly remove them from a contact list and notify PHC IAPO.

Posters, ads

- Submit all posters and ads (visual and oral scripts) with your REB RISe application.
- If you are using QR codes, please contact PHC IAPO in advance of submitting your REB RISe application.

Letter of Initial Contact

- PHC IAPO developed the Letter of Initial Contact (LoIC) template and guidance document to support researchers recruiting PHC patients for the PHC REB and Providence approved studies (available on Providence Research website).
- The LoIC must come from the PHC department that is responsible for that patient information and must be signed by the relevant PHC PCM or designated department staff (not the Physician Department Head) responsible for the patient area from which the patients were seen.
- USE PHC LOGO ONLY. Do not include UBC or any other health authority logos, even for harmonized studies.

Social Media

- Submit all posts and ads (media files and text scripts) with your REB RISe application.
- Please include the following statement on the social media posting: “Please note: If you choose to post about this study on social media, comment, “like”, or “follow” it, you may be identified personally.”

REACH BC

- REACH BC platform is administered and managed by Michael Smith Health Research BC. If you plan to use this recruitment platform in your project, please indicate that in your REB RISe application along with the details on how will you manage the records received and who will have access to them.

Referral

- Please include details about patient's consent to disclose their personal information, personal information included in the referral, how will this information be shared with the research team, who will have access to it, and how it will manage when your project employs patient referrals from third-parties, including HCPs.

3. Participant contact

- Submit all patient contact scripts with your REB RISe application.
- Always document all contact made with and responses from patients and study participants.
- Ensure that a patient is removed from the contact list promptly and alert the PHC IAPO if the patient does not wish to be contacted or if the patient seems upset by the contact. They may be directed to contact the PHC IAPO (604-806-8336 or privacy@providencehealth.bc.ca) or you may also ask the patient if they would like the PHC Privacy Office to contact them about their concern.
- If you become aware or suspect that a communication containing personal information was misdirected, disable any automated follow-up messages, and notify PHC IAPO immediately.

Email

- Use PHC email account. Email addresses issued by another health organization or trusted institution may also be used. The use of personal email accounts (ex. Gmail, Yahoo, Hotmail) is not allowed.
- Authentication must be done prior to the initial email being sent, as per PHC Emailing Policy. Confirm the correct email address in person or over the phone.
- To mitigate risks from misdirected emails, document that a particular email has been authenticated in a study-specific log, copy/paste the address from the file instead of typing it manually, do a final cross check of the emails prior to sending.
- Limit the amount of personal information included in the email. Do not include personal information in the subject line.
- Ensure that the ICF communicates the risks associated with emailing. See section 1. General considerations. Informed consent provisions.

Phone

- Use a PHC-issued device where available. Devices issued by another health organization or trusted institution may also be used. If using a non-PHC issued device, ensure that the device is password protected and that the cloud storage back up is disabled.
- Do not leave detailed or sensitive messages on VM or with third-parties answering the phone.
- If you are using a 3rd party automated reminder calls system, see section Data Management and Electronic Systems for details to be provided.

Texting

- Use a PHC-issued device where available. Devices issued by another health organization or trusted institution may also be used. If using a non-PHC issued device, ensure that the device is password protected and that the cloud storage back up is disabled.
- Authentication must be done prior to the initial text being sent, as per PHC Emailing Policy. Confirm the correct phone number in person or over the phone.
- Limit the amount of personal information included in the text.

- If you are using a 3rd party automated reminder system, see section Data Management and Electronic Systems for details to be provided. Consider using a platform that has been reviewed for privacy and security, such as WelTel Health.

Zoom, MS Teams, 3rd party systems

- Preferred application is PHSA's Zoom for HealthCare or UBC Zoom.
- Microsoft Teams cannot be used for research purposes at this time.
- Participants will need to be notified of risks with using the virtual health tools via the Informed Consent Form.
- If research interviews are being done via third party applications, please see section 1. General Considerations.

4. Transcription Services

Unique voices, names, accents, opinions expressed, etc., that are conveyed and recorded during interviews or focus groups are considered elements of personal information. As such, the use of automated tools may require a Privacy Impact Assessment, please contact PHC IAPO before submitting your REB RISe application.

Automated tools

- Each research study is responsible for their own transcription tool subscription. Consider using a tool that's been reviewed, such as Temi transcription.
- A confidentiality agreement must be signed for each research project.
- A written informed consent must be obtained from a research/ interview participant to authorize the recording of their interview and to inform of the location the audio and text files will be temporarily stored on.
- The transcript is to be downloaded as soon as it is available. Both audio and text files are to be deleted from the platform as soon as the resulting text file is downloaded to limit the duration of time the files are stored on the platform.
- The project team should assign an individual to routinely check the platform account (ie: monthly) to ensure the audio files are deleted. All research data must be stored and retained as required per the approved REB application.
- It is recommended all digital files be stored in encrypted/password protected folders on the PHC's network (VCH, PHSA, and UBC networks are acceptable as well) to limit access to the transcriptions. If digital files are to be shared, secure transfer methods must be used, such as IMITS SFT or UBC OneDrive.

Human Transcriptionists

- Legal agreement and PHC confidentiality undertaking must be signed before any transcription files are exchanged with the transcriptionist.
- It is recommended that the encrypted files are stored and accessed through approved file sharing platforms (ex. UBC OneDrive) and follow the file storage and user access management good practices.
- If files are to be downloaded to a local computer, all cloud-syncing must be disabled. Once the transcription is done double delete the records as soon as possible, document/ acknowledge via email that the deletion is complete.