HREBA | Health Research Ethics Board of Alberta

1500, 10104 - 103 Avenue
Edmonton, Alberta, T5J 0H8

Phone: 780-423-5727
Toll-free: 1-877-423-5727

Regulatory Guidelines Third Party Recruitment and Screening

Guidelines Discussion

Having consulted with the Office of the Information and Privacy Commissioner, HREBA's statement of mandate and obligations related to the review of third-party participant recruitment agencies are confirmed below.

HREBA's mandate and obligations under the *HIA*[1] are in relation to "individually identifying"[2] "health information" (referred to as *IIHI*).[3] Where a researcher intends to conduct research "using health information in the custody or under the control of a *custodian* or *health information repository* [italics added]"[4] they must submit a proposed research protocol to HREBA for review.

If the information being gathered is not in the custody or under the control of a custodian or health information repository, then the *HIA* does not apply to that information. Consequently, where *IIHI* is:

a. being collected by a third-party recruitment agency directly from individuals in Alberta; and
b. that a third-party recruitment agency is not under the control of a custodian (e.g. not acting as an agent or under contract with the custodian).

In such cases, HREBA has no mandate or obligation under the *HIA* to review all the third-party's information collection processes. Accordingly, HREBA will no longer require submission of a third party's recruitment processes or conduct an exhaustive review of those processes in these cases.

However, it must be remembered that the provisions of *TCPS2 2022* remain applicable. Accordingly, "In considering the voluntariness of consent, REBs and researchers should be cognizant of situations where undue influence, coercion or the offer of incentives may undermine the voluntariness of a participant's consent to participate in research."[5] HREBA will continue to review these processes to the extent required to assess whether undue influence, coercion, and/or incentives are involved in the proposed recruitment processes.

---

[1] Alberta *Health Information Act* - RSA 2000, c H-5 | Health Information Act | CanLII (*HIA*), ss. 49-56.
[2] *HIA*, s. 1(1)(p).
[3] *HIA*, s. 1(1)(k).
[4] *HIA*, s. 49. For the definition of a "custodian" or "health information repository" see: *HIA* s. 1(1)(f) *and Health Information Regulation, Alta Reg 70/2001*, s. 2.
[5] *TCPS2 2022*, Chapter 3, Article 3.1, Application section.

1500, 10104 - 103 Avenue
Edmonton, Alberta, T5J 0H8

Phone: 780-423-5727
Toll-free: 1-877-423-5727

Best practice would be to obtain consent that includes all items in the attached Checklist; and, to contact HREBA or the Office of the Information and Privacy Commissioner should any questions or concerns arise.

It should be noted that while HREBA's mandate does not extend to reviewing the third-party recruitment agencies' information collection processes, the third-party recruitment agencies still have obligations to comply with *PIPA*[6] and *FOIP*[7] (and see fn. 7 re non-applicability of *PIPEDA*). Privacy breaches must still be reported to HREBA and to the Office of the Information and Privacy Commissioner. Further, if the third-party recruitment agencies' information collection processes are not compliant with *PIPA or FOIP* one possible consequence is that the Privacy Commissioner may order any collected information to be destroyed following an investigation by the Commissioner. This could have serious implications for ongoing research. If sponsors, researchers, or third-party recruitment agencies have questions or concerns about their obligations under *PIPA or FOIP*, they may consider conducting a Privacy Impact Assessment[8] or contact the Office of the Information and Privacy Commissioner directly.[9]

For collection of *IIHI* from custodians, or where a third-party collection agency is dealing with *IIHI* in the custody or under the control of a custodian, HREBA will consider whether adequate safeguards are in place to protect the privacy of the individuals who are the subjects of the research. In these cases, the third-parties' full information and collection processes must be submitted to HREBA in connection with the proposed research; and, the standard review procedures will apply.[10] As above, if it comes to HREBA's attention that the data that are proposed for use in research have not been collected in compliance with the relevant requirement, HREBA may refuse to approve proposed research or revoke previous approvals.

For the guidance in this area, please see:

Pursuant to the *HIA*, the consent forms must include:

---

[6] Alberta *Personal Information Protection Act* - SA 2003, c P-6.5 | Personal Information Protection Act | CanLII (*PIPA*).

[7] *Freedom of Information and Protection of Privacy Act (FOIP)*. *PIPEDA* is only applicable to provinces and territories that do not have private sector privacy legislation. It does not apply to the Alberta issues being discussed here because of the existence of *PIPA* which has been deemed substantially similar to *PIPEDA* (RSA 2000, c F-25 | Freedom of Information and Protection of Privacy Act | CanLII. Personal Information Protection and Electronic Documents Act - Personal Information Protection and Electronic Documents Act | CanLII (*PIPEDA*).

[8] See Privacy Impact Assessments at https://oipc.ab.ca/privacy-impact-assessments/.

[9] Office of the Information and Privacy Commissioner of Alberta, https://oipc.ab.ca/.

[10] As set out in HREBA's SOPs, TCPS2 2022, GCP, applicable Health Canada, FDA, EMA and similar legislation, applicable regulations, and other related legal and ethical guidelines. See: HREBA Standard Operating Procedures - https://hreba.ca/hreba-cancer-committee/hreba-standard-operating-procedures/ (SOPs); TCPS2 2022 pdf - https://ethics.gc.ca/eng/documents/tcps2-2022-en.pdf (*TCPS2*); ICH-GCP Guidelines - ICH Official web site: ICH (GCP).

1500, 10104 - 103 Avenue
Edmonton, Alberta, T5J 0H8

Phone: 780-423-5727
Toll-free: 1-877-423-5727

1. an authorization for the custodian to disclose *IIHI*;
2. the purpose for the disclosure;
3. who will receive the *IIHI*;
4. an acknowledgment that the participant has been made aware of the reasons why the *IIHI* is needed and the risks and benefits of consenting or refusing to consent;
5. the date the consent is effective and (if applicable) the date the consent expires; and
6. a statement explaining how the consent may be revoked.[11]

Pursuant to *TCPS2* the consent forms must include:

1. the type of information to be collected;
2. the purpose for which the information will be used;
3. risks to participants should the security of the data be breached;
4. appropriate security safeguards;
5. anticipated linkage of data gathered in the research with other data about participants; and
6. whether those data are contained in public or personal records.[12]

CIHR/GCP guidance[13] further requires the proposal and consent forms to:

1. Determine the research objectives and justify the data collection needed to fulfill those objectives.
2. Limit the collection of personal data by ensuring that the information collected is restricted to what is necessary to achieve the research objectives.
3. Anticipate future uses of the data, including possible collaborations with other researchers and/or possible commercial uses.
4. Safeguard data by establishing appropriate institutional policies and procedures including organizational, technological, and physical measures.
5. Control future access to, and disclosure of, personal data (e.g. access by whom, for what purposes, based upon what further approvals, etc.).
6. When personal data are to be entered into a database for multiple research uses over an extended period, research participants should also be informed of such things as: expected types of studies, expected data types and purposes, expected commercial uses, data retention period, and the process for overseeing the use and security of data. Participants may also be given the opportunity to provide authorization for future uses, with or without

[11] *HIA*, s. 34.
[12] *TCPS2*, Article 5.3, Application Section.
[13] CIHR Best Practices for Protecting Privacy in Health Research (September 2005) https://cihr-irsc.gc.ca/e/29072.html; pdf version available at https://cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf; CIHR Privacy Best Practices - 10 elements in Summary Form https://cihr-irsc.gc.ca/e/29072.html#Summary; CIHR Best Practices for Protecting Privacy in Health Research (September 2005) https://cihr-irsc.gc.ca/e/29072.html; pdf version available at https://cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf.

1500, 10104 - 103 Avenue
Edmonton, Alberta, T5J 0H8

Phone: 780-423-5727
Toll-free: 1-877-423-5727

re-contact, including the opportunity to withdraw consent (and any identifying information) in the future.

7. When personal data are collected in a database to support general health research purposes in the future, personal data may be retained for the general purposes originally consented to, subject to security safeguards proportionate to the identifiability and sensitivity of the data.

Finally, all the above requirements are affirmed as regular practice in HREBA's *SOPs*; and, for ease of reference, they have been consolidated in the Compliance Checklist below.

Compliance Checklist[14]

- ☐ The type of *IIHI* to be collected.
- ☐ A determination that the research objectives justify the proposed scope of data collection.
- ☐ The purpose for which the *IIHI* will be used and/or disclosed.
- ☐ Who will receive/have access to the *IIHI* and in what form (e.g. fully identifying, de-identified, anonymized, coded, etc.).
- ☐ Anticipated future uses of the data, including possible collaborations with other researchers and/or possible commercial uses.
- ☐ Statement describing appropriate security safeguards in place, including the establishment of appropriate institutional policies and procedures including organizational, technological, and physical measures.
- ☐ How future access to, and disclosure of, the data will be controlled (e.g. access by whom, for what purposes, based upon what further approvals, etc.).
- ☐ Risks to participants should the security of the data be breached.
- ☐ Anticipated linkage of data gathered in the research with other data about participants.
- ☐ Whether those data, portions of those data, or subsequent linkages to those data, will be contained in public or private records.
- ☐ When *IIHI* is to be entered into a database for multiple research projects uses over an extended period, research participants should also be informed of such things as: expected types of studies, expected data types and purposes, expected commercial uses, data retention periods, and the process for overseeing the use and security of data. Participants may also be given the opportunity to provide authorization for future uses, with or without re-contact, including the opportunity to withdraw consent (and any *IIHI*) in the future.
- ☐ When *IIHI* is collected in a database to support general health research purposes in the future, personal data may be retained for the general purposes originally consented to, subject to security safeguards proportionate to the identifiability and sensitivity of the data.

[14] Note: the protocol and/or consent documents must address all of the following principles that are relevant to the research being undertaken. However, they need not be addressed in the same order as the compliance checklist.

1500, 10104 - 103 Avenue
Edmonton, Alberta, T5J 0H8

Phone: 780-423-5727
Toll-free: 1-877-423-5727

- An acknowledgment that the participant has been made aware of the reasons why the *IIHI* is needed and the risks and benefits of consenting or refusing to consent.
- Authorization for the custodian to disclose *IIHI*.
- The date the consent is effective and (if applicable) the date the consent expires.
- A statement explaining how the consent may be revoked.