Annex 1. Contract Checklist for Cloud-Based Genomic Research
Version 1.0, 21 July 2015

The following comprises a checklist of areas that genomic research organizations or consortia (collectively referred to below as "researchers") should consider before signing, or while negotiating, legal arrangements to store genomic data on one or several cloud service provider's ("CSP's") servers. Migrating genomic and other data to the cloud is part of the evolution of existing technologies and large-scale genome science, but it comes with risks. Therefore, researchers should undertake significant due diligence in order to better understand what cloud computing entails, both prior to data migration and throughout the data life cycle. This means that researchers should assess which data, if any, could be migrated to the cloud, in what form, and according to which processes; which internal safeguards should be developed; how data will be encrypted; and, after concluding a contractual agreement with a CSP, how monitoring of obligations will be conducted.

Cloud contracts can be either non-negotiable, standard-form contracts drafted by the CSP (possibly tailored to specific jurisdictions or sectors (e.g., health)) or negotiated contracts tailored to fit the specific requirements of the researcher. Both types of contracts are generally called Terms of Service ("ToS"), hereinafter used interchangeably with the term "contract" and cover terms and conditions, service-level agreements ("SLAs"), acceptable use policies ("AUPs"), and privacy policies. Sometimes these documents are folded into the ToS, other times they are incorporated by reference.

This checklist is non-exhaustive and serves only as a guidance document. The items listed below are not ranked in order of importance. The information in this document is for the general information of the reader and is not intended as legal advice or opinion to be relied upon in relation to any particular circumstance.

Contractual Form and Applicable Law

- **Term and Termination**
  - Pay attention to the **term** of a cloud contract.
    - Is there a minimum term?
    - Are the ToS in force over a fixed, renewable, or indefinite period?
    - How long is the researcher "locked in"? Until interoperability among CSPs advances to a level of seamless data portability, researchers should aim for flexibility to transition out of the services, and are discouraged from over-reliance or dependence on one CSP, which may have proprietary application programming interfaces ("APIs") (less of a concern with open-source cloud infrastructure).
    - Paid services (including the "pay as you go" model offered by large CSPs) often include clauses that specify the contract will continue indefinitely until termination (whether by convenience or otherwise), and clauses defining breaches by the customer that result in managed or immediate termination of the contract.
  - Be aware of what actions will bring the contract term to an end, e.g., breach of AUP or "inactive account" clause (e.g., 90 days without access).
    - Do the ToS allow or deny the customer a right to access data on termination?
    - Will the CSP assist the researcher to safely migrate data elsewhere?
    - Does the CSP assert a right to terminate the service at its discretion without cause? If so, does it provide reasonable advance notice?
  - If possible, negotiate a reasonable termination notice period in order to have enough time to transition out of the services, migrate data, and possibly applications, to one or several other CSPs. However, because migration may be necessary due to CSP insolvency or winding down, researchers should verify before signing a cloud contract that they are readily able to migrate data in desired formats in whatever notice period they are confident they will be given.
    - Is there a reasonable period of time offered to customers to remedy a breach before termination?

- **Applicable Law**
  - Pay attention to the jurisdictions where the researcher, other end-users, CSP, and data centres will be located.
    - Are the ToS subject to laws in one or more of these jurisdictions?
    - Do any applicable data privacy laws override or limit any clauses in the ToS or prohibit any foreseeable data use?
    - Which adjudication bodies, and in which jurisdictions, govern potential disputes arising out of the contract?
  - Consider whether the CSP mandates its principal place of business as being located in a particular jurisdiction, or instead offers a range of ToS to choose from, allowing the researcher some control over the applicable legal system. Large CSPs may be able to tailor ToS to conform more closely to local legal systems. In most cases, researchers will prefer their own jurisdiction, but if this is not possible, researchers should attempt to ensure that the ToS do not subject them to a jurisdiction that would put data at increased privacy risk.
  - Attempt to secure assurance from the CSP that it has conducted a regulatory review of its own services or terms and that its services are compliant with applicable law.

- **Service Description**
  - Privacy laws in Canada require a "custodian" who transfers personal information to a service provider to specify the limited processes the CSP may carry out with that personal information.
  - Ensure that a service description is explicitly mentioned in the ToS. If a CSP induces a researcher by offering specific, tailored features, they should be fully reflected in the ToS.
    - Does the CSP restrict researchers from using its services for any purpose involving personal information without prior written consent from the CSP?

- **Amendments to ToS / APIs**
  - For paid services and negotiated contracts, changes to the ToS should be restricted to those made in writing with the agreement of the parties.
    - Is the CSP obligated to notify customers regarding changes to APIs or the ToS for a service? If so, what is the process, and is the prior notification period reasonable? How does this period compare with the delay required to migrate to another CSP if necessary?
    - Can the ToS be unilaterally modified by the CSP? If so, must the CSP notify the researcher directly? Is the researcher instead responsible for checking the CSP website for amendments? Is continued use deemed acceptance of the modified terms? Are notifications only given when the CSP determines that the modifications are "material"? Does the website list only the current ToS, or indicate its last change, prior versions, or descriptions of the modifications? Do modifications take effect immediately, or only after a delay?
  - The ToS should allow researchers to terminate the agreement if they do not wish to accept a change.

Data Handling and Safeguards

- **Privacy and Security Safeguards**
  - Know who has the ultimate responsibility for preserving the confidentiality and integrity of data. Some CSPs make customers solely responsible for securing, protecting, and backing up their data. CSPs may make non-binding assurances about measures they will undertake to safeguard researcher data. Others may offer to make "best efforts" or "reasonable and appropriate measures" to secure such data against accidental or unlawful loss, access or disclosure. If possible, and particularly for paid services, ask for binding, explicit details about these safeguards, and avoid agreeing to generic assurances.
  - Examine the CSP's approach to securing and protecting data. This may depend on the type of cloud service offered (e.g., IaaS, PaaS, SaaS).
    - Does data security appear to be a priority? Does the CSP make known that it relies on named open and community-reviewed security standards and platforms, or does it instead aim to achieve security by keeping its processes secret, including from its customers? What are the physical and digital security measures?
    - Is the CSP willing to provide specific documentation (e.g., Cloud Security Alliance certification, ISO 27001, ISO 27002 or ISO 27018 policies and procedures)?
    - Does the CSP make backups? If so, is it included or is it a separate service that requires payment? CSPs that make backups should assume liability for backup integrity and data loss, but it is always recommended that customers make backups themselves.
  - At a minimum, safeguards should meet industry standards such as those of the National Institute of Standards in Technology, the Cloud Standards Customer Council, or the best practices published by the Cloud Security Alliance. Whichever standard is proposed, security specifications should provide comprehensive coverage focusing on technical, administrative and physical safeguards.

- Researchers may want the CSP to adopt supplementary measures identified by the researcher that are appropriate to the data's sensitivity. If accepted by the CSP, these security measures may be scheduled or annexed to the ToS.
- Safeguards should be periodically audited, and the researcher should have audit rights and identify which party bears the expense of such an audit.
- Attempt to have CSPs commit to a general obligation to comply with all relevant privacy laws.
- Researchers may be obliged in some provinces to notify individuals or privacy authorities in the case of a breach involving personal information, and should therefore attempt to contractually obligate the CSP to notify them of any data loss or security breach (that affects the researcher's data) within a reasonable period of time (e.g. <24 hours), and to contain the breach as best as possible. The researcher may also want to negotiate for termination rights if the security breach is significant.
- Try to secure a standalone confidentiality/non-disclosure agreement in an effort to highlight/clarify confidentiality obligations.
- Attempt to secure CSP liability for breach of confidentiality and, if possible, personal information protection obligations generally.

- **Data Location and Transfer**
  - Privacy laws in Canada may prohibit transfer of personal information outside a jurisdiction except in specific circumstances. Researchers in these jurisdictions should not contract with a CSP that declines to include terms to comply with these transfer restrictions.
  - Investigate as much as possible the trail of data storage and transfer, and ensure that a CSP will transfer data only in an encrypted manner over secure networks, and will encrypt data at rest where applicable and practicable.
    - Can the CSP process, store, back up, or temporarily move data to any country where the CSP or its agents maintain facilities? If so, which countries? Does the CSP offer data transit protection?
  - Researchers concerned about the location of their data storage may want to have the CSP agree to transfer data only to specific locations providing an equivalent or greater level of protection for data to that applicable where the data originated. Some CSPs guarantee that data will remain in particular locations of the researcher's choice, even for remote access (i.e., "follow-the-sun" services that use support staff or sub-contractors in other locations to access researcher data or metadata).
  - Ensure flow-through obligations where sub-contracting is used by the CSP (including for support services) through preapproved lists, by obtaining assurance that sub-contractors are contractually bound to the CSP, and/or requiring advance notification or even veto rights before the CSP engages subcontractors.

- **Data Monitoring**
  - See if the CSP can monitor the researcher's data, and if so, in what form and under what conditions.
    - If data is encrypted, does the researcher want the CSP to have access to decryption keys? Monitoring of traffic data or bandwidth consumption may be acceptable, but a researcher could be concerned with a CSP monitoring data uploaded to the cloud, even if the CSP states that such monitoring is to ensure compliance with the accepted use policy or to prevent hosting of illegal or otherwise inappropriate content.
  - Be vigilant as to the extent of a CSP's ability to have "back door" access to their data, be it for maintenance, servicing, support, or even security purposes.

- Researchers may want the CSP to agree to treat any data obtained from monitoring or support or maintenance activities as subject to confidentiality provisions, or to restrict the purposes for which CSPs can monitor data.
- Researchers should apply their own organization's policies for giving authorization/access privileges to CSP employees for certain situations (e.g., emergencies, support).

- **Data Disclosure**
  - Find out if the CSP will or may disclose data when required by law or requested by governmental authorities.
    - Will the disclosures be made with or without prior or subsequent notice (depending on the circumstances)? Does a relevant jurisdiction's law allow the CSP to be prohibited from notifying the researcher that it was compelled to disclose the data? What level of detail will the notice provide about the data that were disclosed?
    - Does the customer have a right to object to or challenge data disclosure?
  - CSPs will almost certainly disclose researcher data in response to a valid court order (though a private international law question arises about whether they will always comply with a court order from a foreign jurisdiction). Take note that many countries (not just the U.S.) have legislation allowing for government access to data for national security purposes upon court order. In this situation, researchers should ensure that the CSP will give them advance notice of the requested disclosure (unless such notice is prohibited), and that the CSP will assist the researcher in opposing the court order. Be informed as to the frequency with which a given jurisdiction exercises these powers, and in what circumstances, to the degree this information is available.
  - Some CSPs may also disclose data in response to *requests* (not necessarily legally binding court orders) from recognized government and law enforcement agencies or where there is a clear and immediate need to disclose information in the public interest.

- **Data Preservation and Deletion**
  - Data preservation and deletion is especially important for genomic research consortia. This is sometimes referred to as "lock-in". Have an exit strategy and plan for end-of-contract transition.
    - What happens to the researcher's data after the relationship with the CSP comes to an end?
    - Can the researcher retrieve the data to move them elsewhere? Does the CSP assure that the data will then be deleted comprehensively (i.e., including duplicates or backups) and securely (i.e., so that the data do not remain retrievable from the physical disk even after they are deleted from the perspective of the operating system) from its servers (and any sub-processors' servers) upon the researcher's retrieval of them?
  - Data deletion after termination should be a top priority for researchers. There will likely be financial costs involved for a CSP to comprehensively delete data.
  - Often data preservation clauses depend on whether the service is paid or free. Free services may not guarantee data preservation. Some CSPs will preserve data for a period of time (grace period) following the end of the cloud contract (e.g. 30 days to 6 months) unless it is terminated for cause, in which case there may be immediate data deletion. Other CSPs may stipulate that they will delete the data immediately upon the end of the ToS, no matter the circumstances. Researchers should not agree to such a clause, and a CSP may be in breach of ToS if the termination was ineffective. The ToS may instead be silent on this point, providing neither a grace period (or one only at the CSP's discretion), nor an undertaking to delete the data. In all cases, ask for clarification of the CSP's data preservation policy regarding how long the grace

period lasts, commitments to comprehensively delete the data, and any additional costs that may be involved.

Warranty and Liability

- **Representations and Warranties**
  - Does the CSP provide any warranty to the customer regarding performance of the service, or claims that the service offerings are provided "as is"? CSPs may deny that any such warranty of service exists, unless required to by local law (e.g., consumer protection laws, which invariably apply only to natural persons and not commercial users or entities such as organizations or consortia).
  - In paid service agreements, however, consider whether to require a warranty that the service will be uninterrupted or error free, or a mechanism for compensation if the CSP fails to deliver the agreed level of service (i.e., in the case of a service outage).

- **Liability**
  - Consider the breadth of the CSP's waiver of liability. Some CSPs, particularly where ToS are governed by the laws of U.S. states rather than European countries, waive all liability for any unauthorized access or use, corruption, deletion, destruction or loss of any data maintained or transmitted through its servers, regardless of who is at fault.
    - How and to what extent does the CSP seek to shield itself from liability arising out of the customer's conduct?
    - Does the CSP exclude **direct liability** for damage caused to the researcher by the CSP (e.g., losses arising from security breaches, data breach or loss, denial of service, performance failures, accuracy of the service)?
      - How is direct liability defined?
      - Does it exclude direct liability for acts of God (extraordinary events or circumstances beyond the control of the CSP)?
      - How is "direct loss" defined?
    - Does the CSP exclude **indirect liability** (e.g., indirect, consequential or economic losses arising from a breach by the CSP)? Invariably, CSPs will seek to exclude liability for incidental losses.
      - How is "indirect loss" or "consequential loss" defined?
    - Does the CSP impose a **limitation of liability** (i.e., maximum amount of damages liable for)? In paid service contracts, most CSPs impose a set maximum limit (e.g., total amount paid by the customer over the previous 3-12 months). In free service contracts, often there is total denial of liability.
  - The CSP should be liable for, at a minimum, willful/gross negligence with respect to data integrity and confidentiality (i.e., intentionally performing an unreasonable act in disregard of a known risk, making it highly probable that harm will be caused). As well, attempt to negotiate for liability for defined types of breach or loss, such as breach of confidentiality, privacy laws, data loss/corruption, or breach of regulatory or security requirements that could give rise to regulatory sanctions.

- **Indemnification**
  - Is the researcher required to indemnify the CSP against any claim against the CSP arising from the customer's use of the service?
  - Researchers should seek mutual indemnification.