FAQs for the EpicCare Link and Hyperspace Access

My organization does not need consent to view and collect the data. Why do I need to sign the agreement?

We acknowledge that some of the organizations to whom we provide access do not require consent to access the data. However, we are required in our agreement with Epic, who owns the licenses to the solution, to impose terms and conditions on organizations accessing the data through Epic's solution. These include general terms and conditions such as respecting Epic's intellectual property and other similar conditions. Additionally, the agreement clarifies the relationship between the parties and includes terms and conditions that are normally found in a data sharing agreement between two organizations.

Is the agreement negotiable?

Generally no. We have developed the agreement with assistance from internal and external legal counsel. We have developed commercially reasonable terms that are relevant to the variety of relationships and organizations to whom we provide access to our system. Due to the volume of organizations with whom we have a relationship, we are generally unable to negotiate the terms of the agreement. However, if there are terms to which an organization is unable to commit by law, the organization should propose alternative language and a rationale for the change.

My organization is not a health information custodian (HIC) under PHIPA. Is this agreement still appropriate?

Yes. The agreement has been developed to accommodate the variety of organizations to whom we provide access and the variety of purposes for which they access the data. There are a number of terms in the agreement that do not apply if the other party is not a HIC under the *Personal Health Information Protection Act* (PHIPA). However, we request that you not strike these out because we have very limited capacity to review changes made by each organization.

Does my organization really need $5,000,000 of cyber insurance?

Yes. We have included this requirement on the advice of our insurers. Cyber insurance covers an organization for privacy and security-related breaches that are not covered by other insurance policies. The amount of $5,000,000 for a significant breach is realistic to cover the cost of containment, investigation, notification, remediation, potential fines/penalties and potential legal action.

Why does the agreement provide The Ottawa Hospital with the right to remove access without notice?

We would strive to notify and work with the impacted organization(s) prior to removing their staff's access. However, there may be instances such as in a privacy or security breach where we need to immediately suspend access to contain the breach before we make the notice.

Who from our organization should sign the agreement?

The agreement needs to be signed by:

a. Someone from the organization that is requesting access. An organization cannot sign on behalf of or sponsor access for end-users from another organization; and
b. Someone who has the authority to bind the organization. In a large organization, this is likely to be an executive team member (e.g., CEO, CFO). In a community-based practice, this is likely the physician lead or the clinic director. However, you will need to identify who in your organization has the authority to sign the agreement.

What should I include in the description column of the attestation?

In one or two bullet points, describe how you meet the requirement. Also note if your organization has an existing policy that addresses this requirement.

Our end-users use Atlas Alliance equipment to access patient information because they work onsite at one of the Atlas Alliance Members. How should we complete the items on the attestation that refer to the security of our devices?

If your end-users work onsite and use Atlas Alliance equipment, please respond "N/A" to those questions where an Atlas Alliance Member provides the technology. Please also note in the description column why it is not applicable (e.g., "Our users will exclusively use Atlas Alliance Member provided devices and networks. The users have been educated and are aware of this requirement.")

Why is drive-level encryption required on devices accessing personal health information?

It is possible for an end-user to save information to their computers via screen shot or other mechanism. Temporary files may also be automatically saved on the computer if the end-user prints documents. Drive-level encryption helps to ensure that the information is protected should the device be lost or stolen.