**Request for Use of Alternative Virtual Platforms at TOH**

If you plan to use a virtual platform outside of TOH’s approved platforms (Microsoft Teams, EPIC Telehealth (currently powered by Zoom), Ontario Telemedicine Network (OTN)), please complete and submit this form to **Alain Audette (TOH Senior Technology Analyst & Audiovisual Team Lead) at** [**aaudette@toh.ca**](mailto:aaudette@toh.ca) **prior to** submission of your REB application. Evidence of approval from the TOH Audiovisual Team will need to be uploaded into the OHSN-REB application.

Please copy Anne Lavigne, Director, TOH Privacy Office at [alavigne@toh.ca](mailto:alavigne@toh.ca) and Marwan Dayfallah, TOH Information Security Officer at [madayfallah@toh.ca](mailto:madayfallah@toh.ca) onto the request.

|  |
| --- |
| **Section 1.0: General Information** |

* 1. Form Date: Click here to enter text.
  2. CRRF ID/OHSN-REB Protocol Number: Click here to enter text.
  3. Protocol Title: Click here to enter text.
  4. Local Principal Investigator: Click here to enter text.
  5. Name of Requestor: Click here to enter text.
  6. Email Address of Requestor: Click here to enter text.

|  |
| --- |
| **Section 2.0: Platform Information** |

* 1. Justification for why the platforms approved for use at TOH (MS Teams, Epic Telehealth powered by Zoom and OTN) will not work for your study:  
      Click here to enter text.
  2. The name of the platform that you intend to use as well as the anticipated retention time for your account (e.g.: 6 months, 1 year, etc.)?  
     Click here to enter text.
  3. Provide a description of how the platform will be used to meet the needs of your work:  
      Click here to enter text.
  4. Indicate who will be contacted through the platform (e.g.: TOH patients, TOH staff, external staff, external research committees, etc.):  
     Click here to enter text.
  5. What type of data will be collected, used, stored, and processed by you and by the vendor and how sensitive is it?   
     Click here to enter text.
  6. Who will have access to the data, and how can we confirm this?  
      Click here to enter text.
  7. Does the vendor claim the right to use the information for its own, secondary purposes?  
      Click here to enter text.
  8. Where does the vendor operate and/or store the data and what laws govern data in that jurisdiction? Are those laws comparable to Canadian privacy laws/GDPR/US Regulations?  
      Click here to enter text.
  9. Do we have a contract with this vendor?  
      Click here to enter text.
  10. Is access to personal information limited and restricted to authorized individuals?  
       Click here to enter text.
  11. What controls does the vendor have in place for intrusion detection, perimeter security,   
       physical security, application of security patches, and data-leak prevention, among other safety   
       measures?  
       Click here to enter text.
  12. Has the vendor done any privacy or security assessments? Are they willing to share an   
       executive summary for review?  
       Click here to enter text.
  13. What policies and procedures are in place to detect, prevent, and mitigate identity theft?  
       Click here to enter text.
  14. How are incidents and breaches reported?  
       Click here to enter text.
  15. Will we receive notification if a breach to our data occurs?  
       Click here to enter text.
  16. Can the data be retrieved and/or permanently deleted from the vendor’s systems and servers?  
       Click here to enter text.

|  |
| --- |
| ***For use by TOH Audiovisual Team ONLY:*** |
| *Date of Approval: Click here to enter text.*  *Name of Approver: Click here to enter text.*  *Signature of Approver:*  *Notes (if applicable): Click here to enter text.* |

|  |
| --- |
|  |