Notes:

1. This is not an exhaustive list of items and should not be considered as *a one size fits all*. Adjustments will be required.
2. These strategies may not be applicable for all organizations.
3. This checklist is not legal advice and should not be used without obtaining the advice of a lawyer first.

Cybersecurity Risk Management Checklist				
Item	**Description**	**Yes**	**No**	**Not Applicable**
		☑	☒	☑
Risk Awareness				
1	Have you created an inventory of your personal health information (PHI) and personal information (PI) data holdings?			
2	Does the inventory include: • a description of the data holding? • identification of the system in which the data holding is located? • who has access to the data holding? • identification of your key data holdings?			
3	Do you have an inventory of your information technology (IT) assets?			
4	Have you conducted: • a privacy impact assessment (PIA) to identify the privacy risks to individuals: i) for whom you act as the health information custodian (HIC) of their PHI; and ii) whose PI you hold? • a threat risk assessment (TRA) and a Vulnerability Assessment (VA) to identify the threats, vulnerabilities and risks to the security and integrity of the PHI and PI? • privacy and security assessments on (medical) devices that are connected to your systems in which PHI and/or PI is stored?			
5	Have you created a risk register that: • documents all the risks identified in #4, with their associated risk treatment plans? • assigns responsibility for the completion and implementation of each treatment plan? • establishes due dates for the completion and implementation of the risk treatment plans? • tracks progress of the risk treatment activities?			

Cybersecurity Risk Management Checklist				
Item	**Description**	**Yes**	**No**	**Not Applicable**
6	Do you have a list of all the third parties (contractors and vendors) that have access to your PHI and/or PI in the course of providing services to your organization?			
Internal Data Governance				
7	Do you have access to subject-matter expertise in privacy, security and information technology?			
8	Have you identified individuals and their responsibilities for privacy, security and information technology in your organization?			
9	Have you developed and implemented: • a security policy with associated procedures that include management of cybersecurity risk? • a Disaster Recovery Policy with associated procedures? • a Business Continuity Policy with associated procedures? • a privacy policy that includes safeguards to protect your organization against cybersecurity risk? • a Data Retention and Destruction policy with associated procedures?			
10	Do you have a schedule for, and do conduct audits of your business processes involving PHI and PI as against legislative requirements and those in your policies and procedures?			
11	Do you have a schedule for, and do update your policies and procedures to accord with: • new legislative requirements? • new orders and guidance issued by the IPC? • changes in industry standards and/or best practices?			
12	Do you have confidentiality agreements with your employees that set out the consequences if they access PHI or PI without authorization?			
13	Do you provide privacy and security training for your employees, tailoring it to their employment responsibilities in relation to PIH and PI?			

Cybersecurity Risk Management Checklist				
Item	**Description**	**Yes**	**No**	**Not Applicable**
		✓	✗	✓
Internal Technical Security Safeguards				
14	Do your technical security safeguards include: • access controls? • anti-virus, anti- malware and anti-spyware software? • identification and authentication of authorized users? • application whitelisting? • application security and O/S patching? [not sure what this is] • network security (e.g. firewalls, secure remote access, vigorous passwords, where possible, isolation of IoT devices)? • encryption of PHI and PI at rest and in transit? • data back up?			
Vendor Risk Management				
15	Have you conducted due diligence on the privacy and security "posture" of your key vendors requiring access to PHI and/or PI?			
16	Have you developed contractual terms that address vendor's responsibilities for privacy and security risk management?			
17	If your vendor requires access to your systems to provide the services, does your contract include provisions related to restrictions and responsibilities for vendor network access?			
18	Do your vendor contracts require them to have cyber liability insurance?			
19	Do you have a contract management process in place to monitor the vendor's compliance with the terms of the contract?			
Privacy Breach Management				
20	Have you developed and implemented a privacy breach protocol that, at minimum, addresses the matters set out in the IPC guidance: *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector?*			
21	Have you conducted "table top" exercises to practice your response as set out in your breach protocol?			
22	Do you keep updated the contact information of the key stakeholders in your protocol?			

Cybersecurity Risk Management Checklist				
Item	**Description**	**Yes**	**No**	**Not Applicable**
23	Do your vendor contracts address their responsibilities to assist with privacy breach management in the event that the breach results from some inaction and/or action on their part?			
Cyber Liability Insurance				
24	Have you considered purchasing cyber liability insurance?			
25	If you are considering purchasing cyber liability insurance, do you understand: • your cyber security risk exposure? • the types of losses you may reasonably suffer and for which you are seeking coverage? • the coverage being offered by insurers? • preconditions for the coverage of losses (e.g. identification and treatment of pre-existing risks; timely notification; use of audit and logging functionality to identify the individuals and the information that was the subject of the breach)			