Appendix F: Printable Clinic Privacy Officer Tasks Checklist

Privacy Documentation	Initial	Annual	Ongoing
Ensure that clinic privacy and security policies and procedures are developed and maintained to remain current.			
Develop or customize privacy and security policies. Involve clinic physicians and staff to ensure understanding and compliance.	✔		
Use established resources as a starting point for clinic policies. Your PIA binder includes the following resources: • Health Information Privacy and Security Manual • Clinic Policies and Procedures • Risk Assessment	✔		
Maintain clinic policies so that they stay current with regulatory requirements.			✔
Require vendors to advise you (as privacy officer) of any changes to their privacy and security policies and procedures during the length of the contract. Review changes provided to ensure adherence to your clinic's policies and procedures and HIA requirements.			✔
Maintain an electronic or paper copy of the clinic PIA(s) in your business records at all times.			✔
Implement and maintain archives and destruction logs. Review the records retention policies.	✔		✔
Create a privacy officer journal and update it chronologically.	✔		✔
Document changes with vendors, administration, practices, staffing, physical security, orientation, etc.	✔		✔

Privacy Awareness of Staff and Other Agents	Initial	Annual	Ongoing
Ensure that the clinic's physicians and affiliates are aware of and have access to the clinic's privacy and security policies and procedures.			
Deliver or organize initial training for new affiliates (for example, staff, volunteers or students) on the HIA and the clinic's policies and procedures.	✔		
Build confidentiality expectations and consequences into employee job descriptions.	✔		✔
Use staff meetings, bulletins, communication logs, in-services and workshops to ensure clinic affiliates are aware of their responsibilities under the HIA.			✔
Deliver or organize annual training refreshers and ongoing training for clinic staff and contractors as best practices change or the HIA is updated.		✔	✔
Ensure clinic vendors and other agents are aware of their responsibilities and duties.			
Deliver or organize initial training for new vendors and contractors on the HIA and the clinic's policies and procedures.	✔		
Give all vendors and other third parties a copy of the clinic's privacy and security policies and procedures and have them sign a declaration to confirm receipt.	✔		
Require vendors to review the clinic's privacy and security policies and procedures annually.		✔	
Advise external vendors when clinic privacy and security policies have changed.			✔

Privacy Compliance Monitoring	Initial	Annual	Ongoing
Ensure the overall security and protection of health information in the custody or control of the clinic.			
Implement and maintain clinic administrative, technical and physical safeguards to protect patient health information.	✔		✔
Undertake regular Clinic Privacy and Security Program reviews to keep your practices current.		✔	✔
Ensure you have the authority, support and resources to do a proper job.	✔		✔
Complete or assist with writing the clinic's PIA.	✔		
Consider the need to update the clinic's PIA periodically to reflect any physical, technical or administrative changes that may affect the collection, use or disclosure of personal health information in the physician's care or control (for example, change in clinic location, undertaking a data migration project or a change in EMR vendors).		✔	✔
Ensure a disclosure log is implemented and used consistently.	✔		✔
Determine if an Information Sharing Agreement (IMA) is necessary (usually required when there is more than one physician at a location).	✔		✔
Protect clinic staff personal information according to the Freedom of Information and Protection of Privacy Act (FOIP) and the Personal Information Protection Act (PIPA).			✔

Privacy Compliance Monitoring	Initial	Annual	Ongoing
Coordinate and facilitate clinic privacy compliance activities. Identify privacy compliance issues and provide training and guidance to clinic custodians and affiliates.			
Have employees sign a confidentiality agreement when they commence employment at the clinic and annually thereafter.	✔	✔	
Before hiring a third-party vendor, check into their security and privacy policies and practices to help ensure confidence that vendors will keep patient information confidential and secure.	✔		
Have vendors that process, store, retrieve or dispose of health information review and execute an Information Manager Agreement.	✔		✔
Oversee the selection, testing, deployment and maintenance of security hardware and software products.	✔		✔
Oversee IT processes including backup schedule, backup restore testing, EMR/ software installation, EMR access authorization and role-based access matrix.	✔	✔	✔
Ensure that appropriate resources required during a systems failure are identified and appropriate contractual arrangements with adequate service levels are in place.	✔		✔
For any incident/breach use the Risk of Harm checklist within the Breach Management Policy.			✔
Review and act on all reports following a privacy incident. Follow steps in the clinic policies.			✔
Stay apprised of HIA developments such as legislation changes, OIPC orders, OIPC rulings on patient complaints.			✔

Primary Point of Contact for Privacy-Inquiries	Initial	Annual	Ongoing
Act as the clinic primary contact in regard to the HIA and clinic privacy and security policies.			
Be familiar with obligations under the HIA.	✔		✔
Make yourself known to the physicians and staff as the primary privacy clinic resource.	✔		✔
Provide clinic physicians and staff with advice regarding HIA compliance.			✔
Respond to requests for access to or correction of health information.			
Answer patient inquiries and questions regarding privacy and clinic practices.			✔
Ensure access and requests are documented consistently.			✔
Ensure expressed wishes of an individual are documented consistently.			✔
Act as the main point of contact in dealings with third parties (Alberta Medical Association, Netcare, OIPC, researchers, regulatory bodies or the police) regarding privacy and security policies, procedures or incidents.			
Document each issue and outcome.			✔
Review research requests and decide if the clinic will disclose health information for research purposes. Enter into a Research Agreement with the researcher per the HIA before disclosure of any health information.			✔
Receive, investigate and respond to complaints with regards to the clinic's collection, use and disclosure of or access to health information.			
Use the Chapter 14 Duty to Notify Health Information Act Guidelines and Practices Manual and other resources as needed to guide your investigation and response.			✔
Conduct investigations into processes and procedures affecting HIA compliance or clinic privacy and security policies.			✔
Document each privacy breach or suspected privacy breach, its investigation, recommendations and lessons learned.			✔