

Privacy Compliance Checklist

Task	Planned Completion	Completed
Familiarize yourself with legislative and regulatory requirements for personal health information protection		
Gain the support of the President/CEO and senior management for privacy compliance		
Prepare a job description for the Contact Person/Privacy Officer		
Appoint a Contact Person/Privacy Officer		
Train the Contact Person/Privacy Officer		
Prepare terms of reference for the Privacy Team		
Assemble a Privacy Team		
Train the Privacy Team		
Conduct a Privacy Gap Analysis		
Develop an action plan for compliance from Privacy Gap Analysis results		
Draft a Privacy Policy (for internal use)		
Draft a Written Statement of Information Practices (for external use) to post and give to patients		
Establish appropriate privacy practices, e.g.:		
◆ purposes for, and practices relating to, collection, use and disclosure		
◆ consent (implied or express), refusal of consent, withdrawal of consent, conditional consent/lock boxes, mandatory and permitted disclosures without consent		
◆ security safeguards (administrative, technical and physical)		
◆ storage, retention, disposal and transfer		
◆ contract and supplier management		

◆ access to health records		
◆ correction of health records		
◆ research		
◆ fundraising		
◆ dealing with privacy breaches		
◆ dealing with complaints		
◆ interaction with the Privacy Commissioner		
◆ documentation		
Train staff and others to adhere to the Privacy Policy and practices		
Draft necessary forms to implement privacy practices (e.g., written statement of information practices, consent form, withdrawal of consent form, consent to disclosure form, request for access to information form, request for correction of information form, employee privacy pledge, privacy clauses and agreements)		
Evaluate which relationships with outside contractors require a privacy agreement, and enter into privacy agreements		
Develop and implement a self-audit program to make sure compliance efforts are working		
Update the Privacy Policy and privacy practices as required		
Issue ongoing privacy awareness reminders and refresher training		
Periodically communicate with staff and the public about your ongoing privacy efforts		
Monitor developments in the law on an on-going basis and make necessary changes		
Conduct a privacy impact assessment when introducing a new practice, database or delivery system involving personal health information		
Consult with legal counsel to ensure appropriate compliance		