IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
1	**Information security policy**		
	• An overarching information security policy, or equivalent, must be developed and implemented in relation to PHI received by CCO under the *Act* .	75	✓
	• require that steps be taken that are reasonable in the circumstances to ensure that the PHI is protected	75	✓
	• undertake organization-wide threat and risk assessments of all information security assets	75	✓
	• information security program to be developed and implemented consisting of administrative, technical and physical safeguards	75	✓
	• the information security program must:	75	
	• effectively address the threats and risks identified	75	✓
	• be amenable to independent verification	75	✓
	• be consistent with established security frameworks and control objectives	75	✓
	• address the duties and responsibilities of agents in respect of the information security program	75	✓
	• the policy must consist of the following control objectives and security policies, procedures and practices:	75	
	• A security governance framework	75	✓
	• ongoing review of the security policies, procedures and practices	75	✓
	• ensuring the physical security of the premises	75	✓
	• include policies and procedures for the secure retention, transfer and disposal of records of PHI including policies and procedures related to mobile devices, remote access and security of data at rest	75	✓
	• establishing access control and authorization	75	✓
	• information systems acquisition, development and maintenance	76	✓
	• for monitoring	76	✓
	• for network security management	76	✓
	• acceptable use of information technology	76	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• back-up and recovery	76	✓
	• information security breach management	76	✓
	• establishing protection against malicious and mobile code	76	✓
	• outline the information security infrastructure implemented by CCO	76	✓
	• require a credible program to be implemented for continuous assessment and verification of the effectiveness of the security program	76	✓
	• address how and by whom compliance will be enforced and the consequences of breach	76	✓
	• stipulate that compliance will be audited	76	✓
	• refer to more detailed policies and procedures developed and implemented to address the requirements for control objectives and security policies, procedures and practices	76	✓
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or any of the security policies	77	✓
2	**Policy and procedures for ongoing review of security policies, procedures and practices**		
	• A policy and associated procedures must be developed and implemented for the ongoing review of the security policies, procedures and practices put in place by CCO	77	✓
	• The policy and procedure must identify:	77	
	• the frequency of the review	77	✓
	• the agent(s) responsible for undertaking the review	77	✓
	• the procedure to be followed in undertaking the review	77	✓
	• the time frame in which the review will be undertaken	77	✓
	• the security policies, procedures and practices implemented by CCO must be reviewed on an annual basis	77	✓
	• In undertaking the review and determining whether amendments and/or new security policies are necessary CCO must have regard to:	77	
	• orders, guidelines, fact sheets and best practices issued by the IPC	77	✓
	• evolving industry security standards and best practices	77	✓
	• technological advancements	77	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• amendments to the Act and its regulation relevant to CCO	77	✓
	• recommendations arising from privacy and security audits, PIAs and investigations into privacy complaints/breaches	77	✓
	• in undertaking the review and determining whether amendments and/or new security policies, procedures and practices are necessary, CCO must have regard to recommendations arising from information security breaches	77	✓
	• whether the security policies, procedures and practices of CCO continue to be consistent with its actual practices	77	✓
	• consistency between the security and privacy policies, procedures and practices	77	✓
	• procedure to be followed in communicating the amended or newly developed security policies, procedures and practices	77	✓
	• procedure to be followed in reviewing and amending the communication materials available to the public	77	✓
	• complying with the policy and its procedures and addressing how and by whom compliance will be enforced and the consequences of breach	77	✓
	• stipulate that compliance will be audited	78	✓
	• policy and procedure for review of security policies and procedures and for secure transfer of PHI	2008 Recom	Not met
3	**Policy and procedures for ensuring physical security of PHI**		
	• A policy/procedures must be developed and implemented addressing physical safeguards implemented by CCO to protect PHI	78	✓
	• physical safeguards shall include controlled access to the premises and to where PHI records are retained	78	✓
	• compliance with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	78	✓
	• stipulate that compliance will be audited	78	✓
	• the premises of CCO be divided into varying levels of security	78	✓
	• in order to access locations within the premises where records of PHI are retained, individuals be required to pass through multiple levels of security.	78	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• require agents to notify CCO at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of the policy or associated procedures	78	✓
	• set out the various levels of access that may be granted to the premises	78	✓
	• this policy must identify the agent(s) responsible for receiving, reviewing, granting and terminating access by agents to the premises and to locations	79	✓
	• the process to be followed and the requirements that must be satisfied includes	79	
	• any documentation that must be completed, provided and/or executed	79	✓
	• the agent(s) responsible for completing, providing and/or executing the documentation	79	✓
	• the agent(s) to whom the documentation must be provided	79	✓
	• the required content of the documentation	79	✓
	• criteria that must set out by the agent(s) responsible for approving and determining the appropriate level of access	79	✓
	• criteria that must be considered by the agent (s) responsible for approving and determining the appropriate level of access must be based on the "need to know" principle and must ensure that access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities. In the event that an agent only requires such access for a specified period, the Policy must establish a process for ensuring that access is permitted only for that specified period	79	✓
	• this policy/procedure must:	79	
	• set out the manner in which the determination relating to access and the level of access is documented	79	✓
	• whom this determination will be communicated	79	✓
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for making the determination	79	✓
	• the required content of the documentation	79	✓
	• address the agent(s) responsible and the process to be followed in providing identification cards, access cards and/or keys to the premises and to locations within the premises	79	✓
	• notify CCO of the theft, loss or misplacement of identification cards, access cards	79	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• outline the safeguards that are required to be implemented as a result of the theft, loss or misplacement of identification cards, access cards and/or keys	79	✓
	• the circumstances in which and the procedure that must be followed in issuing temporary or replacement identification cards, access cards and/or keys and the agent(s) responsible for their issuance	80	✓
	• address the process to be followed in the event that temporary identification cards, access cards and/or keys are not returned	80	✓
	• require agents to notify CCO of the termination of their employment and to return their identification cards, access cards and/or keys	80	✓
	• require that access to the premises be terminated upon the cessation of the relationship	80	✓
	• an agent's supervisor must notify CCO when the agent no longer requires access to location(s) where records of PHI are retained	80	✓
	• agent's supervisor will notify CCO when the agent no longer requires such access	80	✓
	• The policy and procedure must identify:	80	
	• the agent(s) to whom the notification must be provided	80	✓
	• the nature and format of the notification	80	✓
	• the time frame within which the notification must be provided	80	✓
	• the process that must be followed in providing the notification	80	✓
	• the agent(s) responsible for terminating access	80	✓
	• the procedure to be followed in terminating access	80	✓
	• the method by which access will be terminated	80	✓
	• the time frame within which access must be terminated.	80	✓
	• Audits must be conducted of agents with access to the premises of CCO	80	✓
	• identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures	81	✓
	• identify the agent(s) responsible for maintaining such a log	81	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• address where documentation related to the receipt, review, approval and termination of access to the premises at CCO where PHI is retained and the agent(s) responsible for maintaining this documentation.	81	✓
	• address the agent(s) responsible and the process to be followed in identifying, screening and supervising visitors to CCO	81	✓
	• the policy and procedures will set out:	81	
	• the identification that is required to be worn by visitors	81	✓
	• any documentation that must be completed, provided and/or executed by agent(s) responsible for identifying, screening and supervising visitors	81	✓
	• the documentation that must be completed, provided and/or executed by visitors	81	✓
	• address the duties of agent(s) responsible for identifying, screening and supervising visitors	81	✓
	• address the process to be followed when the visitor does not return the identification provided	81	✓
	• address where documentation related to the identification, screening and supervision of visitors will be retained	81	✓
4	**Log of agents with access to the premises of CCO**		
	• a log must be maintained of agents granted approval to access the premises of CCO	81	✓
	• the log must include:	82	✓
	• the name of the agent granted approval to access the premises	82	✓
	• the level and nature of the access granted	82	✓
	• the locations within the premises to which access is granted	82	✓
	• the date that the access was granted	82	✓
	• the identification numbers on the identification cards, access cards and/or keys	82	✓
	• the date of the next audit of access	82	✓
	• the date that the identification cards, access cards and/or keys were returned to CCO	82	✓
5	**Policy and procedures for secure retention of records of PHI**		

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• A policy and procedures must be developed and implemented with respect to the secure retention of records of PHI in paper and electronic format	82	✓
	• identify the retention period for records of PHI in both paper and electronic format	82	
	• records of PHI used for research purposes, CCO must ensure that they are not being retained for a period longer than that set out in the research plan	82	✓
	• records of PHI collected pursuant to a Data Sharing Agreement will not be retained for a period longer than that set out in the Data Sharing Agreement.	82	✓
	• in any event mandate that records of PHI be retained for only as long as necessary to fulfill the purposes for which the PHI was collected.	82	✓
	• require the records of PHI to be retained in a secure manner and identify the agent(s) responsible for ensuring the secure retention of these records	82	✓
	• require agents of CCO to take steps to ensure that PHI is protected	82	✓
	• If a third party service provider is contracted to retain records of PHI on behalf of CCO the policy must address:	82	
	• when records of PHI will be transferred to the third party for secure retention.	82	✓
	• the procedure to be followed in securely transferring the records of PHI to the third party	82	✓
	• the procedure to be followed in securely retrieving the records from the third party	83	✓
	• documentation is required for the transfer of records of PHI to the third party for secure retention (third party to provide written confirmation upon receipt of records of PHI)	83	✓
	• detailed inventory is required for the PHI being securely retained by the third party	83	✓
	• identify the agent(s) responsible for maintaining the detailed inventory and the agent(s) responsible for ensuring that the Template Agreement for All Third Party Service Providers has been executed prior to	83	✓
	• a detailed inventory is required for PHI retrieved by CCO	83	✓
	• written agreement must be executed with the third party containing the relevant language from the Template Agreement For All Third Party Service Provider	83	✓
	• require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	83	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits,	83	✓
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures	83	✓
6	**Policy and procedures for secure retention of records of PHI on mobile devices**		
	• identify whether and in what circumstances, if any, CCO permits PHI to be retained on a mobile device.	84	Not met
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	84	✓
	• set out the circumstances, in which PHI is retained on a mobile device, is permitted.	84	Not met
	• state whether approval is required prior to retaining PHI on a mobile device.	84	Not met
	• If approval is required:	84	
	• a discussion of any documentation that must be completed, provided and/or executed	84	Not met
	• the agent(s) responsible for completing, providing and/or executing the documentation	84	Not met
	• the agent(s) to whom this documentation must be provided	84	Not met
	• the required content of the documentation	84	Not met
	• have regard to orders, factsheets and guidelines issued by the IPC	84	✓
	• the policy and procedure should set out:	85	
	• the manner in which the decision approving or denying the request is documented;	85	Not met
	• the method by which and the format in which the decision will be communicated	85	Not met
	• to whom the decision will be communicated.	85	Not met
	• address the requirements and criteria for making a decision on a request for the retention of PHI on a mobile device	85	Not met
	• prior to approval the agent(s) responsible for making the decision must ensure that de-identified information will not serve the purpose	85	Not met
	• require mobile devices containing PHI to be encrypted as well as password-protected using strong and complex passwords that are in compliance with the Policy and Procedure relating to Passwords	85	✓
	• identify the conditions or restrictions to retain PHI on a mobile device. The agent must:	85	
	• require that a mandatory standardized password-protected screen saver be enabled after a defined period of inactivity	85	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• identify the agent(s) responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected screen saver is enabled	85	✓
	• Be prohibited from retaining PHI on a mobile device if de-identified and/or aggregate information, will serve the purpose	85	Not met
	• De-identify the PHI to the fullest extent possible	85	Not met
	• Be prohibited from retaining more PHI on a mobile device than is reasonably necessary for the identified purpose;	85	Not met
	• Be prohibited from retaining PHI on a mobile device for longer than necessary to meet the identified purpose	85	Not met
	• Ensure that the strong and complex password for the mobile device is different from passwords for the files containing the PHI	86	Not met
	• detail the steps that must be taken by agents to protect the PHI retained on a mobile device	86	✓
	• ensure the PHI on a mobile device in compliance with the Policy and Procedures for Secure Retention of Records of Personal Health Information	86	Not met
	• securely delete PHI retained on a mobile device in accordance with the process	86	✓
	• If CCO does not permit PHI to be retained on a mobile device, the policy and procedures must expressly prohibit the retention of PHI on a mobile device	86	Not met
	• indicate whether or not PHI may be accessed remotely through a secure connection or virtual private network.	86	Not met
	• If CCO permits PHI to be accessed remotely, the policy and procedures must set out the circumstances in which this is permitted	86	Not met
	• identify whether approval is required prior to accessing PHI remotely through a secure connection or virtual private network.	86	Not met
	• If approval is required identify the process that must be followed for making a decision on a request for remote access to PHI	86	Not met

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• address the requirements and criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for remote access.	86	Not met
	• prior to approval require the agent(s) responsible for making a decision to ensure that , namely de-identified and/or aggregate information, will not serve the identified purpose and that no more PHI will be accessed than is reasonably necessary to meet the identified purpose	86	Not met
	• require the agent(s) responsible for making the decision to ensure that the use of the PHI has been approved	87	Not met
	• identify the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated	87	Not met
	• identify the conditions or restrictions with which agents granted approval to access PHI remotely must comply.	87	Not met
7	**Policy and procedure for secure transfer of records of PHI**		
	• A policy and procedures must be developed and implemented with respect to the secure transfer of records of PHI in paper and electronic format.	87	Not met
	• require records of PHI to be transferred in a secure manner and set out the secure methods of transfer in paper and electronic format	87	Not met
	• require agents to use the approved methods of transferring records of PHI	87	Not met
	• outline the procedures that must be followed in transferring records of PHI through each of the approved methods. This includes:	87	
	• a discussion of the conditions pursuant to which records of PHI will be transferred	87	Not met
	• the agent(s) responsible for ensuring the secure transfer	87	Not met
	• any documentation that is required to be completed, provided and/or executed in relation to the secure transfer	87	Not met
	• the agent(s) responsible for completing, providing and/or executing the documentation	87	Not met
	• and the required content of the documentation.	87	Not met
	• whether the agent transferring records of PHI is required to document the date, time and mode of transfer	87	Not met
	• the recipient of the records of PHI	87	Not met
	• and the nature of the records of PHI transferred	87	Not met

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• address whether confirmation of receipt of the records of PHI is required from the recipient	87	Not met
	• the manner of obtaining and recording acknowledgement of receipt of the records of PHI and the agent(s) responsible for doing so	87	Not met
	• outline the safeguards for transferring records of PHI	88	Not met
	• ensure that the procedures and safeguards required to be implemented in respect of the secure transfer of records of PHI are consistent with:	88	
	• Orders, guidelines, factsheets issued by the IPC	88	✓
	• Evolving privacy and security standards and best practices	88	✓
	• require agents to comply with the policy and its procedures and address how compliance will be enforced and the consequences of breach.	88	✓
	• stipulate that compliance will be audited	88	✓
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	88	✓
8	**Policy and procedures for secure disposal of records of PHI**		
	• A policy and procedures must be developed and implemented with respect to the secure disposal of records of PHI in both paper and electronic format	88	✓
	• require records of PHI to be disposed of in a secure manner and provide a definition of secure disposal that is consistent with the Act	88	✓
	• identify the precise method by which records of PHI in paper format are required to be securely disposed of	88	✓
	• ensure that the method of secure disposal adopted is consistent with:	89	
	• the Act and its regulation	89	✓
	• with orders, factsheets, and guidelines issued by the IPC	89	✓
	• address the secure retention of records of PHI pending their secure disposal	89	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• In the event that records of PHI will be securely disposed of by a designated agent, who is not a third party service provider the policy and procedures must identify:	89	
	• the designated agent responsible for securely disposing of the records of PHI	89	✓
	• the responsibilities of the designated agent in securely disposing of the records	89	✓
	• the time frame, circumstances and the conditions the records of PHI must be securely disposed of	89	✓
	• the designated agent to provide a certificate of destruction	89	✓
	• address where certificates of destruction will be retained and the agent(s) responsible for retaining the certificates of destruction.	90	✓
	• detail the procedure to be followed by CCO securely transferring the records of PHI to the third party for secure disposal	90	✓
	• require the agent(s) responsible for ensuring the secure transfer of records of PHI to maintain a detailed inventory related to the securely disposed records	90	✓
	• require a written agreement where a third party service provider is retained to securely dispose of records of PHI	90	✓
	• outline the procedure to be followed in tracking:	90	
	• tracking the dates that records of PHI are transferred for secure disposal	90	✓
	• tracking the dates that certificates of destruction are received	90	✓
	• whether from the third party service provider or from the designated agent that is not a third party service provider	90	✓
	• the agent(s) responsible for conducting such tracking	90	✓
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	90	✓
	• stipulate that compliance will be audited	90	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	91	✓
	• agreement with third-party service providers who are retained to destroy records should include:	2008 Recom	
	• A certificate of destruction	2008 Recom	✓
	• Signed by the person who performed the destruction	2008 Recom	✓
	• Date, time, location and method of destruction	2008 Recom	✓
	• services will be performed in a professional manner, in accordance with industry standards and practices and by properly trained employees and agents	2008 Recom	✓
	• that a breach of security and confidentiality of the information may lead to disciplinary measures	2008 Recom	✓
	• If the services of another third party will be used it is required that CCO be notified in advance and that the third-party be required by written contract to comply with all the same terms and conditions as the third-party service provider; it is required that a copy of the written contract be provided to CCO .	2008 Recom	✓
9	**Policy and procedures relating to passwords**		
	• A policy and procedures must be developed and implemented with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by CCO	91	✓
	• identify the required minimum and maximum length of the password, the standard mandated for password composition and any other restrictions imposed on passwords	91	✓
	• the frequency with which passwords must be changed, the consequences arising from a defined number of failed log-in attempts and the imposition of a mandatory system-wide password-protected screen saver after a defined period of inactivity	91	✓
	• address the time frame within which passwords will automatically expire	91	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• identify the administrative, technical and physical safeguards that must be implemented by agents in respect of passwords	91	✓
	• ensure that the policy and procedures it has developed in this regard, are consistent with:	91	
	• any orders, factsheets, and guidelines issued by the IPC	91	✓
	• with evolving privacy and security standards and best practices	91	✓
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	91	✓
	• stipulate that compliance will be audited	91	✓
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	92	✓
10	**Policy and procedures for maintaining and reviewing system control and audit logs**		
	• A policy and procedures must be developed and implemented for the creation, maintenance and ongoing review of system control and audit logs.	92	✓
	• must be consistent with evolving industry standards	92	✓
	• must be consistent with the number and nature of agents with access to PHI and with the threats and risks associated with the PHI	92	✓
	• require CCO to ensure that all information systems involving PHI have the functionality to log access, use, modification and disclosure of PHI	92	✓
	• set out the types of events that are required to be audited and the nature and scope of the information that must be contained in system control and audit logs	92	✓
	• identify the agent(s) responsible for ensuring that the types of events that are required to be audited are in fact audited and that the nature and scope of the information that is required to be contained in system control and audit logs is in fact logged	92	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• CCO must be required to ensure that the system control and audit logs cannot be accessed by unauthorized persons or amended or deleted in any way	92	✓
	• the system control and audit logs set out:	92	
	• the date and time that PHI is accessed	92	✓
	• the date and time of the disconnection	92	✓
	• the nature of the disconnection	92	✓
	• the name of the user accessing PHI	92	✓
	• the network name or identification of the computer through which the connection is made	92	✓
	• the operations or actions that create, amend, delete or retrieve PHI	92	✓
	• the policy and procedure will:	92	
	• identify the length of time that system control and audit logs are required to be retained	92	✓
	• the agent(s) responsible for retaining the system control and audit logs	92	✓
	• where the system control and audit logs will be retained	92	✓
	• address the review of system control and audit logs including:	93	✓
	• the agent(s) responsible for reviewing the system control and audit logs	93	✓
	• the frequency with which and the circumstances in which system control and audit logs are required to be reviewed	93	✓
	• the process to be followed in conducting the review.	93	✓
	• The agent(s) responsible for reviewing system control and audit logs shall be required to notify CCO of a privacy/security breach	93	✓
	• address the findings arising from the review of system control and audit logs	93	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• addresses the agent(s) responsible for assigning other agent(s) to address the findings arising from the review of system control and audit logs, for establishing timelines to address the findings , for addressing the findings and for monitoring and ensuring that the findings have been addressed	93	✓
	• the policy and procedure will set out :	93	
	• the nature of the documentation following the review of system control and audit logs	93	✓
	• the agent(s) responsible for completing, providing and/or executing the documentation	93	✓
	• the agent(s) to whom the documentation must be provided	93	✓
	• the time frame within which the documentation must be provided	93	✓
	• the required content of the documentation	93	✓
	• communicating and addressing the findings of the review including the agent(s) responsible for communicating the findings of the review of system control and audit logs; the mechanism and format for	93	✓
	• tracking the findings of the review of system control and audit logs	93	✓
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach	93	✓
	• stipulate that compliance will be audited	93	✓
	• notify CCO if an agent believes there may have been a breach of this policy or its procedures.	93-94	✓
11	**Policy and procedure for patch management**		
	• A policy and procedures must be developed and implemented for patch management	94	✓
	• identify the agent(s) responsible for monitoring the availability of patches on behalf of CCO	94	✓
	• identify the agent(s) responsible for determining whether or not the patch should be implemented	94	✓
	• where the patch should not be implemented the responsible agent is required to:	94	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• document the description of the patch	94	✓
	• the date that the patch became available	94	✓
	• the severity level of the patch	94	✓
	• the information system, technology, equipment, resource, application or program to which the patch relates	94	✓
	• the rationale for the determination that the patch should not be implemented	94	✓
	• where the patch should be implemented the responsible agent(s) shall determine the time frame, and priority of the patch.	94	✓
	• set out the process for patch implementation	94	✓
	• the policy and procedures will address:	94	✓
	• the circumstances in which patches must be tested	94	✓
	• the time frame within which patches must be tested	94	✓
	• the procedure for testing	94	✓
	• the agent(s) responsible for testing	94	✓
	• documentation that must be completed for testing	94	✓
	• documentation to be maintained of patches that have been implemented and identify the agent(s) responsible for maintaining this documentation.	94	✓
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	95	✓
	• stipulate that compliance will be audited	95	✓
	• notify CCO if an agent believes there may have been a breach of this policy or its procedures.	95	✓
12	**Policy and procedures related to change management**		
	• A policy and procedures must be developed and implemented for determining the approval or denial of a request for a change to the operational environment of CCO	95	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• identify the agent(s) responsible and the process that must be followed for making this determination	95	✓
	• identify the criteria that must be considered when deciding to approve or deny a request for a change to the operational environment	95	✓
	• the policy and procedure will:	95	
	• set out the manner in which the decision approving or denying the request for a change to the operational environment	95	✓
	• document the reasons for the decision	95	✓
	• set out the method and the format in which the decision will be communicated	95	✓
	• set out to whom the decision will be communicated	95	✓
	• where a request for change to the operational environment is not approved, it is required to:	95	
	• document the change to the operational environment requested	95	✓
	• the name of the agent requesting the change	95	✓
	• the date that the change was requested	95	✓
	• the rationale for the determination that the change should not be implemented	95	✓
	• where a request for change to the operational environment is approved, the responsible agent is required to:	96	
	• determine the time frame for implementing the change	96	✓
	• the priority assigned to the change requested	96	✓
	• the policy and procedure will:	96	
	• set out the criteria upon which these determinations are to be made	96	✓
	• the process by which these determinations are to be made	96	✓
	• any documentation that must be completed, provided and/or executed in this regard	96	✓
	• the process for implementation of the change to the operational environment	96	✓
	• the agent(s) responsible for implementation	96	✓
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for implementation.	96	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• identify the circumstances in which changes to the operational environment must be tested	96	✓
	• the time frame within which changes must be tested	96	✓
	• the procedure for testing	96	✓
	• the agent(s) responsible for testing	96	✓
	• the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.	96	✓
	• require documentation to be maintained of changes that have been implemented	96	✓
	• identify the agent(s) responsible for maintaining this documentation	96	✓
	• compliance with the policy and its procedures and how compliance will be enforced and the consequences of breach.	96	✓
	• stipulate that compliance will be audited	96	✓
	• require agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	96	✓
13	**Policy and procedures for back-up and recovery of records of PHI**		
	• A policy and procedures must be developed and implemented for the back-up and recovery of records of PHI	96	✓
	• The policy will:	97	
	• identify the nature and types of back-up storage devices maintained by CCO	97	✓
	• the frequency with which records of PHI are backed-up	97	✓
	• the agent(s) responsible for the back-up and recovery of records of PHI	97	✓
	• the process that must be followed and the requirements that must be satisfied in this regard	97	✓
	• specify the documentation that must be completed, provided and/or executed for the back-up and recovery of records of PHI; the agent (s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation	97	✓
	• address testing the procedure for back-up and recovery of records of PHI	97	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• the agent(s) responsible for testing	97	✓
	• the frequency with which the procedure is tested	97	✓
	• the process that must be followed in conducting such testing	97	✓
	• identify the agent(s) responsible for ensuring that back-up storage devices containing records of PHI are retained in a secure manner,	97	✓
	• the location where they are required to be retained and the length of time that they are required to be retained	97	✓
	• require that the backed-up records of PHI must be retained in compliance with the Policy and Procedure for Secure Retention of Records of PHI and identify the agent(s) responsible for ensuring they are retained in a secure manner	97	✓
	• if a third party service provider is contracted to retain backed-up records of PHI, the policy and associated procedures must:	97	
	• require the backed-up records of PHI to be transferred in a secure manner	97	✓
	•detail the procedure to be followed in:	97	
	• securely transferring the backed-up records of PHI to the third party	97	✓
	• securely retrieving the backed-up records from the third party	97	✓
	• ensuring the secure transfer and retrieval of the backed-up records	97	✓
	• address the documentation that is required to be maintained in relation to the transfer of backed-up records of PHI	97	✓
	• the secure transfer shall document the date, time and mode of transfer	97	✓
	• maintain a repository of written confirmations received from the third party upon receipt of the backed-up records of PHI	97	✓
	• execute a written agreement with the third party	97	✓
	• identify the agent(s) responsible for ensuring that the agreement has been executed prior to transferring the backed-up records of PHI to the third party	98	✓
	• address the need for the availability of backed-up records of PHI	98	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	98	✓
	• stipulate that compliance will be audited	98	✓
	• agents to notify CCO if an agent believes there may have been a breach of this policy or its procedures.	98	✓
14	**Policy and procedures on the acceptable use of technology**		
	• A policy and procedures must be developed and implemented outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by the prescribed person or prescribed entity	98	✓
	• sets out the uses that are prohibited without exception, the uses that are permitted without exception, and the uses that are permitted only with prior approval	98	✓
	• For those uses that are permitted only with prior approval, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request and the process that must be followed and the requirements that must be satisfied in this regard.	98	✓
	•the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request	98	✓
	• identify the conditions or restrictions with which agents granted approval must comply.	98	✓
	• the policy and procedures should:	98	
	• set out the manner in which the decision approving or denying the request	98	✓
	• the reasons for the decision are documented	98	✓
	• the method by which and the format in which the decision will be communicated	98	✓
	• whom the decision will be communicated.	99	✓
	•require agents to comply with the policy and its procedures and address how and by whom compliance will be enforced and the consequences of breach.	99	✓
	• stipulate that compliance will be audited	99	✓
	• require agents to notify CCO at the first reasonable opportunity, if an agent breaches or believes there may have been a breach of the Policy or its procedures	99	✓
15	**Policy and procedures in respect of security audits**		

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• A policy and procedures must be developed and implemented that sets out the types of security audits that are required to be conducted	99	✓
	• the audits required to be conducted shall include :	99	
	• audits to assess compliance with the security policies, procedures and practices implemented by CCO	99	✓
	• threat and risk assessments	99	✓
	• security reviews or assessments	99	✓
	• vulnerability assessments	99	✓
	• penetration testing	99	✓
	• ethical hacks and reviews of system control and audit logs	99	✓
	• The policy and procedure must set out:	99	
	• the purposes of the security audit	99	✓
	• the nature and scope of the security audit	99	✓
	• the agent(s) responsible for conducting the security audit	99	✓
	• the frequency with which and the circumstances in which each security audit is required to be conducted.	99	✓
	• set out the process to be followed in conducting the audit	99	✓
	• discuss the documentation that must be gathered for each security audit	99	✓
	• the agent(s) responsible for completing, providing and/or executing the documentation	99	✓
	• the agent(s) to whom this documentation must be provided	99	✓
	• the required content of the documentation.	99	✓
	• the role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program	100	✓
	• the process that must be followed in addressing the recommendations arising from security audits	100	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• the nature of the documentation that must be gathered at the conclusion of the security audit	100	✓
	• the manner and format in which the findings and status of security audits are communicated	100	✓
	• a log be maintained of security audits	100	✓
	• the agent(s) responsible for maintaining the log	100	✓
	• tracking that the recommendations arising from the security audits are addressed within the identified time frame	100	✓
	• the agent(s) responsible for conducting the security audit to notify CCO at the first reasonable opportunity of an information security or privacy breach	100	✓
	• address where documentation related to security audits will be retained and the agent(s) responsible for retaining this documentation.	100	✓
16	**Log of security audits**		
	• maintain a log of security audits that have been completed. The log shall set out:	100	
	• the nature and type of the security audit conducted	100	✓
	• the date that the security audit was completed	100	✓
	• the agent(s) responsible for completing the security audit	100	✓
	• the recommendations arising from the security audit	100	✓
	• the agent(s) responsible for addressing each recommendation	100	✓
	• the date that each recommendation was or is expected to be addressed	100	✓
	• the manner in which each recommendation was or is expected to be addressed.	100	✓
17	**Policy and procedures for information security breach management**		
	• A policy and procedures must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of information security breaches and must provide a definition of the term “information security breach.”	101	✓
	• an information security breach shall be defined to include a contravention of the security policies, procedures or practices implemented by the prescribed person or prescribed entity	101	✓
	• mandatory requirement on agents to notify CCO of an information security breach	101	✓
	• the policy and procedure shall identify:	101	

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• the agent(s) who must be notified of the information security breach or suspected breach	101	✓
	• provide contact information for the agent(s) who must be notified	101	✓
	• stipulate the time frame within which notification must be provided	101	✓
	• whether the notification must be provided verbally and/or in writing	101	✓
	• the nature of the information that must be provided upon notification.	101	✓
	• the documentation that must be gathered with respect to notification	101	✓
	• the agent(s) to whom this documentation must be provided	101	✓
	• the required content of the documentation	101	✓
	• require a determination to be made:	101	
	• whether an information security breach occurred	101	✓
	• if PHI was breached	101	✓
	• of the extent of the information security breach and whether the breach is an information security breach or privacy breach or both	101	✓
	• The agent(s) responsible for making these determinations	101	✓
	• address the process to be followed where the breach is a privacy breach and a information security breach	101	✓
	• address the process to be followed when the breach is reported as an information security breach but is determined to be a privacy breach.	101	✓
	• address when senior management will be notified	101	✓
	• the policy and procedure shall require:	101	
	• that containment be initiated immediately	101	✓
	• identify the agent(s) responsible for containment	101	✓
	• the procedure that must be followed in this regard	101	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• reasonable steps are taken in the circumstances to ensure that additional information security beaches cannot occur through the same means.	101	✓
	• The agent(s) responsible and the process to be followed in reviewing the containment measures implemented and determining whether the information security breach has been effectively contained	102	✓
	• any documentation that must be completed, provided and/or executed by the agent(s) responsible for reviewing the containment measures	102	✓
	• the agent(s) to whom this documentation must be provided	102	✓
	• the required content of the documentation.	102	✓
	• the HIC or other organization that disclosed the PHI to CCO to be notified when PHI is or is believed to be stolen, lost or accessed by unauthorized persons	102	✓
	• the agent(s) responsible for notifying the HIC or other organization	102	✓
	• the format of the notification	102	✓
	• the nature of the information that will be provided upon notification	102	✓
	• whether any other persons or organizations must be notified of the information security breach	102	✓
	• the agent(s) responsible for investigating the information security breach	102	✓
	• the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections)	102	✓
	• the process that must be followed in investigating the information security breach.	102	✓
	• the agent(s) responsible for assigning other agent(s) to address the recommendations	102	✓
	• establishing timelines to address the recommendations	102	✓
	• address the recommendations	102	✓
	• that the recommendations are implemented within the stated timelines	102	✓
	• the documentation be completed, provided and/or executed at the conclusion of the investigation of the information security breach	102	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• a manner and format in which the findings of the investigation of the information security breach are communicated	103	✓
	• a log be maintained of information security breaches	103	✓
	• the agent(s) responsible for maintaining the log	103	✓
	• to track and ensure the recommendations arising from the investigation of information security breaches are addressed	103	✓
	• address where documentation related to security breaches will be retained	103	✓
	• the agent(s) responsible for retaining this documentation.	103	✓
	• agents to comply with the policy and its procedures	103	✓
	• address how and by whom compliance will be enforced and the consequences of breach	103	✓
	• stipulate that compliance will be audited	103	✓
	• amend the Information Security Incident Response Policy	2008 Recom	
	• one person to report to in cases of an information security incident	2008 Recom	✓
	• format and information reported on to report the security incident	2008 Recom	✓
	• consider whether the information security incident involves the unauthorized collection, use, disclosure, retention or disposal of PHI in violation of the Act and its regulation	2008 Recom	✓
	• include notification to the HICs where there are security incidences involving PHI	2008 Recom	✓
	• responsible person for assigning individuals to implement the recommendations, timelines and ensuring that the recommendations are being implemented	2008 Recom	✓
18	**Log of information security breaches**		
	• CCO shall maintain a log of information security breaches setting out:	103	
	• The date of the information security breach;	103	✓
	• The date that the information security breach was identified or suspected;	103	✓
	• The nature of the PHI that was the subject matter of the breach and the nature and extent of the information security breach;	103	✓

IPC 2011 Triennial Review - Requested Security Documentation			
Req.	**Minimum Content of Required Documentation**	**Page Ref# in Manual**	**Req't Met**
	• The date that the information security breach was contained and the nature of the containment measures;	103	✓
	• The date that the HIC or other organization that disclosed the PHI to CCO was notified	103	✓
	• The date that the investigation the breach was completed;	104	✓
	• The agent(s) responsible for conducting the investigation;	104	✓
	• The recommendations arising from the investigation;	104	✓
	• The agent(s) responsible for addressing each recommendation;	104	✓
	• The date each recommendation was or is expected to be addressed	104	✓
	• The manner in which each recommendation was or is expected to be addressed.	104	✓