SUMMARY OF IPC/O's PHIPA DECISIONS (current to January 14, 2018)

The orders and decisions are colour-coded by theme:

Blue – Vendor issues **Yellow** – Snooping or rogue employees **Grey** – Closing a practice **Green** – Access and Correction

Purple – Information management practices **Orange** – Deceased person's records Red – Unauthorized Use or Disclosure White – Recipient rules

Pink – Collection

# and year	Allegations/Facts	IPC Decision
H0-0001 2005	IPC notified by a reporter that X-ray and ultrasound records were raining from skies on a 9-11 film shoot in Toronto. Health records had been sent for recycling instead of shredding by a Toronto health clinic (independent health facility) after a mix up with the driver taking extra boxes away (outside usual shredding bins). Shredding company was also a recycling company – they sold records to a film crew as scrap paper.	The HIC was ordered to review its information practices to ensure compliance with PHIPA and to enter into written contracts with its agent(s) to ensure the secure destruction of PHI, which is the irreversible destruction of the records. The agent paper disposal company was ordered to enter into written contracts with any third parties who are HICs to ensure compliance with PHIPA and to ensure that records containing PHI are kept separate from records that are designated for recycling. Notice to affected patients was through a public post at the clinic.
H0-002 (same hospital as H0-010) 2006	A patient notified a hospital in Ottawa that her ex-husband and his new girlfriend worked at the hospital and she didn't want them to know about her admission. The girlfriend was a nurse and was not providing care to the patient. The emergency department staff did not take steps to formally secure the electronic record. The nurse looked at the records 10 times and disclosed the patient's PHI to the patient's estranged husband. 3 of those viewings happened even after a VIP privacy notice was put on the electronic record after the patient's initial privacy complaint. The estranged husband phoned the	The HIC was ordered to: - Review and revise its practices, procedures and protocols relating to PHI and privacy, and those relating to human resources, including the implementation of a protocol to ensure that immediate steps are taken upon notification of an actual or potential breach to prevent unauthorized access to, use and disclosure of PHI. - Ensure that its agents are informed of their duties under PHIPA and their obligations to comply with the revised information practices of the HIC. The HIC was urged to issue an apology to the patient. The IPC commented that privacy policies are not enough – staff must be trained.

# and year	Allegations/Facts	IPC Decision
	patient and raised the issue of her chronic heart condition.	
H0-003 2006	CPSO called the IPC because health records containing PHI were abandoned by a walk in medical and rehabilitation clinic in Etobicoke when it closed its practice. This included physio, massage therapy records and finance and sign-in sheets.	The HIC, who abandoned the records, was ordered to: - Retain, transfer or dispose of the records in a secure manner, to enter into a written contract if a storage company is used to ensure the secure retention, transfer and disposal of the records and to ensure that access is provided to the affected individuals. - If operating a group of health care practitioners now or in the future, to put practices and procedures in place to safeguard records of PHI, to designate a contact person to facilitate compliance with PHIPA, to enter into written contracts with its health care practitioners setting out the obligations of both parties regarding records of PHI and to make available to patients, in the event of a closure, how the records of PHI will be retained or disposed of and how to obtain access to those records.
H0-004 2007	Hospital physician researcher in Toronto left a hospital laptop in his car and covered it with a blanket. The car was broken into and the laptop was stolen. The laptop was unencrypted and contained the PHI of nearly 2900 current and former hospital patients.	HIC ordered to: - Develop or revise and implement policies and procedures to ensure that records of PHI are safeguarded and that its information practices comply with PHIPA. - Develop "a comprehensive corporate policy that, to the extent possible and without hindering the provision of health care, prohibits the removal of identifiable PHI in any form from the hospital premises. To the extent that PHI in identifiable form must be removed in electronic form, it must be encrypted." - Develop an encryption policy for mobile computing devices, a policy relating to the use of virtual private networks, a privacy breach policy, and to educate staff regarding the policies how to secure the information contained on mobile computing devices. - Review and revise its research protocols and applications to comply with PHIPA (use of PHI for research purposes).

H0-005 2007	An individual notified a reporter that he had viewed an image of a toilet in a washroom on his vehicle's back up camera while driving by a clinic. The reporter hired an investigator to confirm. They parked near the clinic and saw a video image of a patient using a toilet. Patient was attending a methadone clinic in Sudbury and the image had been accessed by the wireless mobile rear-assist parking device ("back up camera"). The clinic had a wireless surveillance camera in the washroom to ensure that the urine samples provided for drug testing were from the correct source without tampering. The wireless camera footage was being beamed out and was intercepted by this back up camera wireless device.	The HIC: - Contained the privacy breach by immediately turning off the wireless system and replacing it with a more secure wired system. - Posted a notice to advise patients of the privacy breach. - Notified the CPSO. - The HIC was ordered to conduct an annual security and privacy review of its PHI handling systems and procedures to ensure continued compliance with the Act.
H0-006 2009	A member of the media notified the IPC that records containing PHI were found scattered on the street outside a medical centre housing a medical laboratory in Ottawa. A parking attendant who was working in the adjacent lot noticed that records had fallen out of a recycling truck as it was leaving the premises. Records included laboratory reports and patient receipts affecting 10 patients. Included patient names, physician names, health care numbers and clinical test results.	The HIC was ordered to: - Implement its plan to place cross-cut shredders in every location. - Ensure that all contracts or agreements in place with third party shredding companies comply with the requirements set out in HO-001, binding the shredding company to the requirements of PHIPA and its contractual agreement with the HIC. Including secure disposal and not recycling.
H0-007 2010	An unencrypted USB memory stick containing PHI was lost by a public health nurse employed by a regional municipality in Durham on her way from an immunization clinic. More than 80,000 individuals were affected. The information included names, addresses, phone numbers, dates of birth, health card numbers, health history and H1N1 vaccination information.	The HIC was ordered to: - Ensure that records of PHI are safeguarded at all times, specifically by ensuring that any PHI stored on any mobile devices (e.g. laptops, memory sticks), is strongly encrypted. - Revise its written information practices in order to comply with and incorporate the requirements of PHIPA and its regulations. - Take the necessary administrative steps to ensure that H1N1 immunization clinics cease collection of the health card numbers of

		individuals attending these clinics, as well as PHI pertaining to priority group status. (They were collecting too much information) - Take the necessary administrative steps to ensure that health card numbers collected from individuals who have attended H1N1 immunization clinics are securely destroyed as well as any PHI relating to priority status collected from individuals after the H1N1 vaccine was made widely available to the general public. The IPC recommended that the Ministry of Health and Long-Term Care with the Chief Medical Officer of Health request all public health units to review the encryption of their mobile devices and receive an attestation from each public health unit that no unencrypted health information is transported on mobile devices. The public was notified through public advertisements in newspapers.
H0-008 2010	Hospital nurse in Toronto left an unencrypted hospital laptop in her car and it was stolen. More than 20,000 patients affected. The laptop had PHI saved on the hard drive including information about hospital incident reports, operating room lists, research data sets, class lists for patient education sessions, patient names, medical record numbers, types and dates of surgeries and physician information.	The HIC was ordered to: - Immediately develop and implement practices to ensure the records of PHI stored on mobile devices ae safeguarded at all times. - Enhance education and awareness programs, and to develop and implement comprehensive, ongoing, role-based privacy and security training pertaining to the risks posed by the deployment and use of mobile devices. - Develop and implement a comprehensive corporate policy and accompanying procedures relating to the secure retention of records of PHI on all mobile devices (e.g. laptops, memory sticks, PDA's). o Any PHI on a mobile device must be strongly encrypted o The Information Management Department is to be charged with the responsibility to ensure encryption software on mobile devices is properly deployed before issuing devices to staff. o CIO has the responsibility to receive immediate notice of any encryption error message and investigate same. o Guidelines must exist for staff receiving new mobile devices. Staff must review and purge all PI and PHI to be transferred to new device. - Conduct a review of all hospital policies to ensure that clear direction is provided when records of PHI are being removed from its premises on mobile devices.

		- Enhance education and awareness programs, and to develop and implement comprehensive, ongoing, role-based privacy and security training pertaining to the risks posed by the deployment and use of mobile devices. The IPC stated "sever all personal identifiers or encrypt the data on mobile devices – Full Stop."
H0-009 2010	Patient requested copies of 34 pages of her psychological therapy notes from her physician in private practice. Doctor agreed to provide patient with access to her records on the condition that she pay a fee of $125, which he calculated using the Ontario Medical Association Guide.	IPC concluded that the fee charged by the doctor for access to the complainant's records of PHI exceeds "reasonable cost recovery". IPC also concluded that the OMA Guide was unreasonable and used the calculations from a proposed regulation for fees. Doctor was ordered to reduce his fee of $125 to $33.50, which represents a "reasonable cost recovery". He did not have to waive the fee.
H0-010 (same hospital as H0-002) 2010	A patient of a hospital in Ottawa complained that a Diagnostic Imaging Technologist (technologist) who was not providing care to the patient accessed her records. The technologist was the patient's husband's ex-wife. She looked at the patient's record 6 times over 9 months including viewing screens with "Sensitive Warning Flags" (although on one occasion she did not go past the sensitive warning flag).	The HIC was ordered to: - Review and revise its policies, procedures and information practices relating to PHI to ensure that they comply with the requirements of PHIPA and its regulations - Amend its Process for Investigating Privacy Breaches and/or Complaints to add a provision requiring an agent who has contravened PHIPA to sign a confidentiality undertaking and non-disclosure agreement - Provide a written report of the privacy breach and a copy of the Order to the technologist's professional college - Issue a communiqué to all agents regarding Orders 2 and 10 which must include a message that the hospital views breaches of this nature seriously, that action will be taken to discipline agents who are found to have breached PHIPA, and that their professional regulatory college will be provided written reports setting out the circumstances of the breach - Include a discussion of Orders 2 and 10 in all future training programs - Conduct privacy retraining for all agents in the technologist's department, as required by the hospital's policy - Amend its written public statement to include a description of the "VIP Warning Flag" system, to indicate how an individual may request one and to identify the employee(s) of the hospital to whom the request may be directed

		- Ensure that the "VIP Warning Flag" may be applied in all electronic information systems that include PHI - Until role-based functionality is instituted, implement a notice that automatically displays whenever an agent logs into a database containing records of PHI and reminds them that they may only access PHI on a need-to-know basis, that access will be tracked, and that failure to comply may result in termination. With a "accept" or "cancel" option for staff to choose. The IPC recommended that the hospital: - Conduct a review of existing technological safeguards and solutions that are currently available on the market to facilitate role-based access and audit - Review the audit functionality on all systems employed at the hospital and take steps to ensure that the audit capability is "turned on"
H0-011 2011	Cancer Care Ontario couriered screening reports for the Colon Cancer Check program via Canada Post's Xpresspost courier service for delivery to the physicians of individuals who were participating or were eligible to participate in the program. 3 physicians did not receive their screening reports – related to 2,388 patients. The reports were believed to have been lost by Canada Post.	CCO is not a HIC but is subject to the Act as a prescribed person. IPC determined that CCO had not taken the steps that were reasonable in the circumstances to ensure the secure transfer of the records of PHI contained in the Screening Reports. The IPC found that CCO had available to it more secure, electronic options for the transfer of the screening reports to physicians. Thus, the alternative, of sending the screening reports to physicians in paper format, was unacceptable. CCO proposed to develop a secure online web portal to delivery screening reports. CCO was ordered to: - Discontinue the practice of transferring screening reports containing PHI to primary care physicians in paper format - Provide a full report on the advantages and disadvantages of transferring the screening reports in electronic format via the OntarioMD web portal, as compared to the proposed CCO web portal - Review the *CCC Privacy Breach Management Procedure* and any related policies and procedures to clarify and ensure that those having an employment, contractual or other relationship with CCO are fully aware

		of their responsibility to immediately report any privacy breaches, suspected privacy breaches and/or privacy risks to appropriate individuals at CCO with responsibility for privacy issues; and - Conduct additional training with those having an employment, contractual or other relationship with CCO to ensure that they are fully aware of their duties and responsibilities under the *CCC Privacy Breach Management Procedure.*
H0-012 2014	Complaint from two patients that a chiropody clinic did not respond to a request for access to health records.	IPC concluded that the HIC refused the complainants' request for access. HIC was ordered to provide a response to the request for access to records of PHI and without recourse to a time extension.
H0-013 2014	A hospital in Scarborough reported two breaches of patient privacy involving allegations that hospital employees used and disclosed the PHI of mothers who had recently given birth at the hospital for the purposes of selling or marketing Registered Education Savings Plans (RESPs). Affected more than 14,000 patients.	The HIC was ordered to: - In relation to all of the hospital's electronic information systems, implement the measures necessary to ensure that the hospital is able to audit all instances where agents access PHI on its electronic information systems, including the selection of patient names on the patient index of its Meditech system. - In relation to the Meditech system: o Work with the Hospital's Hosting Provider to review and amend the service level agreement between the Hospital and the Hosting Provider to clarify the responsibility for the creation, maintenance and archiving of user activity logs generated by the Hospital's use of its Meditech system, and ensure that the user activity logs are available to the Hospital for audit purposes. o Work with Meditech or another software provider to develop a solution that will limit the search capabilities and search functionalities of the Hospital's Meditech system so that agents are unable to perform open-ended searches for PHI about individuals, including newborns and/or their mothers, and can only perform searches based on the following criteria: health number, medical record number, encounter number, or exact first name, last name and date of birth. - Review and revise its Privacy Audits policy, the Pledge of Confidentiality policy and the Pledge of Confidentiality, and the Privacy Advisory and take steps to ensure that it complies with the Privacy Audits policy. - Develop a Privacy Training Program policy, a Privacy Awareness Program policy, and a Privacy Breach Management policy.

		- Immediately review and revise its privacy training tools and materials.
		- Using the privacy training materials developed in accordance with Order provision 5:
		  o immediately conduct privacy training for all agents in clerical positions in the Hospital; and
		  o conduct privacy training for all other agents by June 16, 2015.

H0-14 2015	Hospital charged a lawyer $117 for a copy of the lawyer's client's 112-page health record. Hospital originally wanted to charge $200. Patient said fee was excessive.	The IPC concluded that HICs are only entitled to charge "reasonable cost recovery" and $117 was excessive. It does not matter if the request relates to "access" or "disclosure" – the issue is reasonable cost recovery. Allowed to charge $53.
Decision 15 2015	A psychologist was asked to make a correction to a Custody and Access Assessment Report prepared at the request of legal counsel for parents of a child. Complainant was a parent. Psychologist said he was an independent assessor and not a HIC in this case.	The IPC concluded the psychologist was not a HIC in this case. Therefore, no right to request correction.
Decision 16 2015	A physician's former spouse made a complaint to both the CPSO and IPC about his conduct. Privacy concern was that physician had looked at his ex-spouse's medical records without consent and used against her in a court proceeding. Physician requested a deferral of IPC review of complaint until CPSO resolved companion complaint.	IPC confirmed that the privacy complaint would go forward without further delay and would not wait for CPSO conclusion.
Decision 17 (includes an order) 2015	A hospital received a request for access to records relating to the birth and death of an infant and the care given to the mother and child at the hospital. The complainant was the father of the infant (who had his wife's permission to act for her as well). The request involved both a PHIPA access request and a freedom of information (FIPPA) access request to all records including anything outside the traditional health records of the infant and mother and about him as a	IPC determined that most of the records at issue were "records of personal health information" or records of personal information to which the individuals had a right of access subject to exceptions. However, IPC upheld many of the hospital's decisions to refuse access on the basis of exclusions and exemptions under FIPPA. The public interest override did not apply. The IPC ordered the hospital to reduce the fees charged (did not require a fee waiver) and ordered the hospital to provide access to some records the hospital wished to withhold.

	complainant (including management of his complaint to the hospital and response to lawsuit, email communications by staff, minutes of board meetings, letters and memos of employment-related matters involving staff, documents sent to the CPSO, CNO and coroner as well as quality of care information reports and solicitor client privileged documents).	
Decision 18 2015	A hospital received a request for records relating to the complainant's son, who had died as a result of a motor vehicle accident. The hospital provided responsive records but the complainant believed there should be additional records (such as urine tests and urine analyses) that the hospital had not provided. The hospital replied that they could not find any further records.	IPC required the hospital to provide an affidavit explaining the searches performed and steps taken to locate responsive records. IPC concluded that the hospital had completed a "reasonable search".
Decision 19 (reviewed in Decision 25) 2016	A complainant made a request to the MoHLTC for his deceased brother's medical records. He wanted a list of the names of the medical practitioners who submitted OHIP claims for his deceased brother prior to his death by apparent suicide.	"Access" is different than "disclosure". On death, the right of "access" is exercised by an estate trustee or a person who has assumed responsibility for the administration of the deceased's estate. The complainant was neither. The estate trustee had not given consent to disclose the information to the complainant. A HIC has discretion under PHIPA to disclose PHI about a deceased person under certain circumstances (s. 38(4)). When asked to disclose records to someone other than the estate trustee, a HIC must consider whether it will exercise its discretion and in so doing must base its decision on proper considerations and not in bad faith or for an improper purpose. Individuals can file complaints with the IPC if they are denied information when a HIC decides not to exercise its discretion in s. 38(4) and the IPC will consider whether the HIC relied on proper considerations. In this case, the MoHLTC acted reasonably in exercising its discretion not to disclose PHI.

Decision 20 (this is likely the same family as Decision 19) 2016	A complainant made a request to a hospital for PHI about his deceased brother. The complainant wanted the hospital to release the information to him in order to make decisions about his own need for care. Complainant was not the estate trustee and did not have the consent of the estate trustee. The hospital did not disclose records. The hospital directed the complainant to obtain the estate trustee's permission.	See Decision 19. IPC concluded that the complainant had not provided sufficient information to the hospital to establish that he "reasonably required" the PHI to make decisions about his own health care. The hospital offered to have the complainant work with his doctor to explain why he needed the deceased brothers' health information.
Decision 21 (includes an order) 2016	A complainant asked for disclosure by a hospital for PHI of his deceased sister. He wanted records for when she received treatment for mental illness at the hospital. Complainant was not the estate trustee and did not have the consent of the estate trustee. The hospital declined to disclose to the complainant. It did not think the psychiatric records would be helpful for the complainant to make decisions about his own health care because psychiatric records could not be used for purposes of analysis of biological, pathological or DNA samples to be genetically mapped and analysed for familial traits and epidemiological tracking.	See Decision 19. IPC concluded that the hospital did not properly exercise its discretion to disclose under s. 38(4). The hospital was ordered to re-consider. The IPC concluded that the hospital took an unduly narrow approach to s. 38(4)(c). The section does not only relate to "specimens". Information about mental illness could be "reasonably required" by a family member. The IPC recommended that the complainant and other family members provide additional details as to why the mental health information was reasonably required by them in order to make their own health care decisions.
Decision 22 (includes an order) 2016	A complainant asked for disclosure by a CCAC of PHI of her deceased mother. Complainant asked for the mother's health records for the last 7 months of her life. She wanted access on compassionate basis as she needed to cope with her grief. Parts of the record were verbally read to the complainant. She had been a contact for her mother before her mother's death. Complainant was not the estate trustee and did not have the consent of the estate trustee.	See Decision 19. IPC concluded that the CCAC did not properly exercise its discretion to disclose under s. 38(4). The CCAC was ordered to re-consider its discretion to disclose under s. 38(4)(b)(ii) and (c). Compassionate disclosure of details of the circumstances of death is reasonable under that section. However, the IPC did not think that the mother's medical conditions in the 7 months leading to her death is all related to the "circumstances of death". The IPC recommended that the complainant provide additional details as to why the

	The CCAC declined to disclose further information to the complainant.	mental health information was reasonably required by her in order to make her own health care decisions. Consent to act as a contact person prior to death did not give the complainant any right to her mother's information after death.
Decision 23 (includes an order and see Decision 28 for resolution) 2016	A group of health care providers went bankrupt and abandoned their practices and their records. The landlord was left with abandoned health records on its premises.	The IPC issued an interim order directing the landlord of the premises holding the abandoned records to ensure the security of the records for 2 months (until the IPC completed a review).
Decision 24 (includes an order) 2016	Request to the City of Ottawa for PHI from the health unit. Request under PHIPA and MFIPPA. Request for access to client intake discharge forms, public health nurse notes, email correspondence and hospital mobile crisis team referral. The public health unit gave the majority of the records but withheld portions.	There was some confusion over who is the custodian with respect to a municipal public health unit. Some records were rightly withheld because of solicitor-client privilege and to protect the identity of a confidential source. A few records did not meet the test to protect the identify of a confidential source and the HIC was ordered to grant access to certain records and portions of other records on that basis.
Decision 25 (review of Decision 19) 2016	MoHLTC objected to the IPC's jurisdiction over complaints about the refusal to disclose PHI of deceased family members.	IPC concluded there were no grounds for reconsideration of the IPC's jurisdiction to receive complaints about the wrongful exercise of the discretionary power to disclose.
Decision 26 2016	A patient objected to paying a doctor $825 for a 141-page "medical-legal report". The patient wanted to pay only the $65 copying fee.	The IPC concluded that a fee charged for creating a medical-legal report is not a fee governed by PHIPA. The doctor was able to charge whatever fee he wanted. Creating a medical-legal report is not the same as providing a "straight copy" of a medical record, which fee would have been governed by the Act.
Decision 27 2016	A woman made a 911 call for medical assistance for her uncle (who since died). She wanted a copy of the audio recording of her call. She asked the Toronto Police Services and then the Toronto Paramedic	The record of the 911 call was a record of PHI. But, the complainant was not the estate trustee and therefore did not have a right to access the record. The record of the call was not the complainant's information. Making a call or supplying information to a HIC does not entitle a third person to access that information at a later date. There was not enough PI of the complainant in

	Services (of the City of Toronto). The city denied the request. This was an MFIPPA and PHIPA complaint.	the call to justify severing the record to provide the PI content to her under MFIPPA.
Decision 28 (continuation of Decision 23) 2016	All patient files abandoned by the three bankrupt corporations had been secured. Steps had been taken to ensure all individuals will be able to access their records	The interim order of Decision 23 concluded. New HICs took over the vast majority of abandoned records. Regulatory Colleges retrieved the remaining records and will protect them. The landlord was no longer required to store and protect the records.
Decision 29 2016	Former patient of a deceased doctor did not want his records sent or kept by a medical records storage company and did not want the records converted from paper files to electronic files. Complainant alleged that the storage company was holding the records "ransom" because there was a fee to have a copy of the records.	When a physician dies, the physician's estate trustee becomes the HIC. The estate trustee is allowed to engage a medical records storage company to keep the records – but the medical records storage company does not become the HIC. The storage company is allowed to convert paper records to electronic copies and does not have to keep the original paper records.
Decision 30 (same family as Decision 33) 2016	A hospital received a request for access to PHI by the deceased patient's daughter for records of a meeting. The hospital denied access to two records on the basis of solicitor-client privilege.	The IPC concluded that the records were records of PHI – but access was rightly denied on the basis of solicitor-client privilege.
Decision 31 (includes an order) 2016	Physician received a request for access to PHI by deceased patient's son. 5 months later, the physician had not responded to the request. The physician did not respond to the IPC's requests for a response (over an 8-month period).	Although there was no estate trustee, the requestor was one of four people who had taken over administration of the estate of the deceased and the other 3 consented to the access. IPC ordered physician to provide a response to the requestor (and with no further time extension) within one week.
Decision 32 (same family as Decisions 38 and 45) 2016	A hospital received a request for access to a child's health records. The parents made a complaint to the IPC that the hospital did not respond to the request within the 30-day required timeframe. The actual timing of viewing the records happened 36 days after the request for access.	IPC concluded there were no grounds for a review by the IPC. The hospital's response was sufficient because the hospital sent a letter within the 30-day period to set up a meeting to view the record. The parents had an opportunity to view the record. This decision provides details about when the 30-day period starts and what kind of communications count as providing a response.

Decision 33 (same family as Decision 30 – includes an order) 2016	A hospital received a request for access to PHI by deceased patient's daughter (and for her own information). This involved both a FIPPA and PHIPA request. Daughter had initiated a lawsuit against the hospital. Daughter had also initiated complaints to regulatory Colleges, MoHLTC, Accreditation Canada and Ombudsman's office. Daughter was joint estate trustee and had consent of other estate trustee.	IPC ordered HIC to disclose parts of two records but generally upheld hospital's refusal to grant access records. Hospital rightly did not provide access to: - Records of quality of care information under QCIPA - Records protected by solicitor-client and litigation privilege including communications about the various legal proceedings commenced by the daughter, draft correspondence to the daughter and outside regulatory bodies circulated for review and comment, internal summary of legal advice, updates on various litigation matters, patient relations office documents including chronology of events and compilation of concerns raised by complainant But hospital had to release parts of records of internal communications between hospital staff on preparing responses to the complainant (most of which had already been shared)
Decision 34 2016	A mental health facility received a request for access to PHI The notes included an interdisciplinary progress note and case conference note totally approximately 113 pages. The facility refused to provide access on the grounds of risk of harm to his nursing staff.	HIC must demonstrate a risk of harm that is well beyond the merely possible or speculative (but a HIC does not have to prove that disclosure will result in harm). This mental health facility was allowed to deny access based on a risk of harm based on the patient's treating psychiatrist's opinion that the patient would likely misinterpret the records and incorporate the content into his delusional beliefs which could affect nursing staff and result in possible violence against the nursing staff who had authored the records.
Decision 35 2016	The daughters of a deceased patient lodged a complaint to the CPSO against their mother's physician about his prescribing practices. Six months after the death, the physician asked a pharmacy for a copy of the prescription summary for the mother and the pharmacy sent a summary of the prescriptions issued by the doctor. Both the pharmacy and the physician were aware of the patient's death. The daughters complained to the IPC that the pharmacy could not send the information to the physician and	HICs cannot have consent of a patient to share information after the patient's death. There is no circle of care after death. But sharing of PHI after death between a physician and pharmacist was allowed without consent of the estate trustees for reasons of quality of care and to disclose information to a regulatory College. Because there was a CPSO review of the physician, it was reasonable for the pharmacy to disclose information to the physician in furtherance of quality of care considerations.

	the physician could not receive information from the pharmacy.	
Decision 36 2016	A patient asked a hospital to make 66 corrections to a 9-page psychological report prepared 15 years before by a physician. Patient asked for changes related to number of admissions to hospital, name of program of study, reasons and duration of psychological testing, description, duration and impact of medical episodes of psychiatric history, reasons for hospitalization, timing of specific events in patient's parents' relationship and type of abuse suffered; and other requests.	Hospital agreed to correct the date of birth. IPC concluded that the psychological report was not inaccurate or incomplete and contained professional opinion or observation made in good faith. No additional corrections were required.
Decision 37 2016	A hospital received a correction request to make 10 changes to a psychiatrist's 1-page discharge summary. Patient requested changes to diagnosis and presenting problems. The record related to a stay 20 years earlier.	Hospital agreed to change the incorrect date of birth. IPC concluded that the discharge summary contained the physician's good faith professional opinions or observations and the hospital did not have to make additional changes to correct the record.
Decision 38 (same family as Decisions 32 and 45) 2016	A hospital received privacy complaints about the hospital's information practices from parents of a patient. 9 incidents were raised: (1) staff collected information about the patient in a hallway within earshot of others; (2) hospital did not charge the parents for a copy of the daughter's health record and hospital did not give mother a copy of an administrative form; (3 and 4) hospital staff left the mother in a diagnostic imaging room unattended and disclosed the patient's records to the father after he produced only the patient's health card and the records were unencrypted when provided to the parents; (5) hospital Health Records staff discussed the parents' request for a copy of health records in a	IPC concluded there was nothing to investigate or review. The hospital admitted in the case of issues 3 and 4 that hospital staff should have followed the hospital's identification authorization practices and agreed to tighten their processes. In the case of issue 5, the hospital agreed to remind staff not to use white out correction fluid on authorization forms. The IPC stated that in issue 5 the release of information to the parents could have been a technical breach of privacy but for the fact that the daughter had given her parents permission to pursue issues with the hospital on her behalf and the hospital had had many dealings with the parents on this file prior to the daughter turning 16 and the parents had not raised the issue at the time. With respect to issue 6, the hospital agreed that in future the Access to Information and Privacy Officer would close his door during meetings.

	small office where others could overhear the conversation and staff used white out correction fluid to make a change to a document on an authorization form and did not ask parents for daughter's consent to release information to them; (6) the Access to Information and Privacy Officer left the door open when speaking with the parents and did not ask to see the parents' identification before speaking with the; (7) an electronic signature on an electrocardiogram demonstrates that a physician viewed the record without authorization; (8 and 9) multiple copies of the diagnostic imaging disks were made and distributed to third parties and the parents were able to access confidential documentation of the hospital demonstrating that hospital staff were not careful with information.	
Decision 39 2017	A hospital received a correction request for a 2-page discharge summary written 20 years ago by a psychiatrist. The request related to: date of birth; description of living arrangements; description of the reason for the admission to hospital; mental state and history for two weeks prior and two years prior to admission; the author's physical examination notes; description of the medical testing and medicine administered during hospitalization; and diagnosis.	The hospital agreed to change the date of birth and description of the complainant's living arrangements. The hospital's decision not to correct the rest of the record was upheld because the record reflects the author's professional opinion made in good faith..
Decision 40 2017	A physician received a correction request to change 26 portions in four letters he sent to the complainant about the termination of the doctor-patient relationship. The issue was whether the statements were actually the physician's "opinion" or whether they were factual information.	The letters terminating the relationship were found to be records of personal health information. The physician's decision to not correct the records was upheld. The complainant was not able to prove the information was inaccurate for the purposes for which the custodian uses the information.

Decision 41 2017	A hospital received a correction request to change the date of a record of a visit to the emergency department. The complainant states he went to a walk-in clinic on a specific date and was told to go to emerg. He says he went to emerg that date and not six days later which is the date indicated on the record at issue. He provided evidence (emails and voice messages) that he told others he had gone to emerg on the same date as the walk-in clinic visit. He wanted the hospital to produce back up tapes to the electronic system to find his attendance. He states the hospital maliciously switched his records with another patient's information.	The hospital's decision to not correct the record was upheld. The record was automatically electronically date stamped and there had been no tampering. The hospital was able to provide additional information to prove the patient had been there on the date stamped by the electronic system. The complainant was not able to prove the record was inaccurate or incomplete for the purposes for which the information is used.
Decision 42 (same physician as HA11-55) (includes an order) 2017	A physician received an access request but did not respond and did not provide a notice of an extension of time. IPC was involved to mediate. Requests for access dated back five and six years (with no response). Patient made a new request because timeframe within which to complain had expired. Physician still did not provide access. The physician was no longer practicing.	IPC ordered the no-longer practising physician to provide a response to the request for access. Physicians do not cease to be a HIC until complete transfer of custody and control of records to another person legally authorized to hold the record.
Decision 43 2017	A hospital received a correction request to change a consultant's report by adding information about his overnight stay, changing a family member's history of addiction to present tense, change a description of the individual's appearance and behaviour, change the description of the individual's cognitive function and challenge the diagnosis. The hospital agreed to change a small portion of the report but not all the requested changes because the record reflected professional opinion made in good faith. Patient also complained that the hospital failed to locate a fax	The hospital's decision to not correct the record was upheld. The hospital had conducted a reasonable search for the missing fax from the family physician.

	from his family physician and claimed the hospital failed to execute a "reasonable search".	
Decision 44 2017 Includes an order	A patient of a hospital (who was also a physician working in the radiology department) alleged that his work colleagues used and disclosed his health information without his permission and without lawful authority. He alleged they looked at his radiology images in the PACS system for personal interest and not as part of providing him with care. Audits showed that colleagues had scrolled through his images as part of reviewing their worksheets. The hospital responded that scrolling activity was not a "use" or viewing of the records.	The IPC concluded that the allegations were unsubstantiated, with one exception where one physician colleague of the complainant was found to have used more information than was necessary for the purpose. The hospital was ordered to improve its privacy training about not using more personal health information than necessary (s. 30). The IPC also recommended that the hospital (1) improve its auditing capabilities to distinguish between scrolling through radiology worklists and viewing reports in the PACS system; (2) investigate whether they could log print commands of PACS; and (3) investigate automatic timed logout in PACS to prevent unauthorized access.
Decision 45 (same family as Decisions 32 and 38) 2017	A hospital received a correction request from parents of a patient. There were multiple corrections requested of a record relating to a single visit at the hospital which lasted one hour. The hospital made four changes but refused to make the remaining requested corrections on the basis that the record was accurate and complete and consisted of professional opinions or observations made in good faith. The additional correction requests had to do with clinical notations in the record such as references to "tearing chest pain" and "thoracic pain" among others. Among other concerns, the parents stated their daughter had not experienced the symptoms listed in the records and the parents alleged the hospital committed fraud by intentionally including incorrect information in the record. The parents also alleged that relevant clinical information was not noted in the records – information that would have showed the hospital did not provide proper care (such	The hospital's decision not to make further corrections to the record was upheld. The IPC concluded that some of the allegations did not raise issues of incompleteness or inaccuracy. The IPC stated that some of the allegations made by the parents fell outside the jurisdiction of the IPC (including issues of failure to meet standards of practice and treatment as well as the allegations of fraud). The IPC also responded to the parents' concerns that the IPC was biased in favour of the hospital.

	as missing notations of failure to keep their daughter well hydrated).	
Decision 46 2017	A physician received a correction request to change two entries in clinical notes. The physician made some changes but denied the other correction requests. Physician felt the requested changes reflected a disagreement about the use of pronouns and syntax. Physician felt the additional requests were frivolous or vexatious or that the complainant had not established that the records were incomplete or inaccurate.	The physician's decision not to correct the record was upheld. IPC discussed the meaning of "frivolous" and "vexatious". IPC found that the request was not frivolous or vexatious (burden on custodian to prove). But concluded that the complainant had not proven that the records were incomplete or inaccurate.
Decision 47 2017	A hospital received a correction request to change references in two consultation reports to specific diagnoses and medication compliance because they were "no longer true". Complainant acknowledged they had been true at the time the diagnoses and notes of medication compliance were recorded. The hospital denied the correction request.	IPC concluded that a review was not warranted. The complainant did not establish that the records were incomplete or inaccurate.
Decision 48 2017	A hospital received a request for access to records. The hospital provided the complainant with a full copy of his health records but the complainant believed there should be additional records (specifically letters from a social worker) that the hospital had not provided. The complainant had copies of the letters the social worker had written and wanted confirmation that the hospital had those letters in its records. The social worker had since retired from the hospital. The hospital searched for those records, but could not find them.	IPC required the hospital to provide affidavits explaining the searches performed and steps taken to locate responsive records. IPC concluded that the hospital had completed a "reasonable search" and was convinced the hospital did not have copies of the social worker letters.
Decision 49	After a clinical appointment, a patient took a photograph of a physician's computer screen. The	IPC concluded that the photograph was a record of personal health information and that the physician had disclosed personal health information

2017 Includes an order	image captured the health information of 71 other patients. The patient was upset that the physician had left the computer unlocked with his and other people's information on the screen. He wanted to pursue a legal claim against the physician and was threatening to make the image public or share the image with his lawyer in order to file a lawsuit against the physician or both. Once notified of the photograph, the physician asked the patient to securely destroy it because he was not authorized to have the other patients' information. The patient refused. The physician notified the 71 patients of the privacy breach. And worked with the IPC. The IPC will review the physician's practices separately.	to the patient by not protecting the information on the computer screen. The disclosure was not authorized by PHIPA. IPC found that the patient was a "recipient" of personal health information under PHIPA. As such, the IPC had the authority to and ordered the patient to destroy the image and all copies because the patient had or intended to contravene PHIPA. Because the patient had not yet initiated legal action against the physician many months later, the IPC refrained from deciding whether the patient would have been entitled to use the image for the purposes of litigation. The hospital undertook to maintain a copy of the image in case of future litigation.
Decision 50 2017	A group medical clinic and a departing physician had a dispute over who was the health information custodian and whether an EMR service provider should have allowed the departing physician to extract his patients' health records. The matter went to court and resulted in a consent order granting the physician ongoing access to his patients' records held by the clinic. The clinic complained to the IPC that the EMR service provider improperly transferred patient files to the departing physician.	The IPC decided not to engage in a review. The court had been involved and the parties agreed to a consent motion. The IPC did not need to be involved and any ongoing issues of dispute should be managed through the court process. However, the IPC commented on the importance of proactively establishing who is the health information custodian in multi-party relationships like group medical clinics. The IPC referred to its document "How to Avoid Abandoned Records" and referenced the responsibility to clearly identify the custodian. The IPC also advised that agreements with EMR service providers should clarify who is the custodian and who can authorize record extractions.
Decision 51 2017	An individual complained that a registry (prescribed person under PHIPA) sent her a letter with another person's laboratory results. A mix up occurred with laboratory results relating to two individuals with the same first name and last name and date of birth.	The IPC decided a review was not warranted. In conducting its investigation, the IPC concluded the mistake was not a labeling error by the referring physician. Instead, it was a rare matching error (linking logic) by the registry (because one of the two individuals did not have an OHIP number). The registry was encouraged to look for opportunities to prevent this rare mistake from happening again.

Decision 52 2017 Includes an order	A hospital received an access request to all the "underlying electronic data about him held by the hospital, in its native, industry-standard electronic format, including data files produced by diagnostic equipment". The hospital provided copies of the patient's records producible through available queries – but objected to having to create new systems to provide native format raw data. The hospital raised objections at the possible cost implications of having to provide raw source data in native format to all patients. The patient also questioned whether the hospital conducted a "reasonable search".	The IPC concluded that the complainant was not entitled to access data in the hospital's electronic systems, devices or archives that could not be extracted through custom queries against reporting views available to the hospital. There was no obligation to produce patient data in its "native format". The IPC discussed the difference between "data" and "information" and concluded that patients' rights of access apply to both. But, the IPC concluded that the electronic databases in which the patient's information was found were not dedicated primarily to his information. Each database pooled information together with other patients. And this patient's information was not easily severable from the other patients' data. The IPC concluded some of the data requested was not even reasonably available to the hospital. In citing *McInerney v. McDonald*, the IPC stated that a patient has a right to access the same information viewed by or available to those providing health care. Not more data/information that the hospital itself could not reasonably utilize through reporting views available to it. On the topic of the "reasonable search" the IPC supported the hospital's search practices and acknowledged that this case was "novel". The hospital was ordered to (1) issue or confirm a fee estimate and (2) provide information available in one database and (3) do a further search of its "billing" records.
Decision 53 2017 Includes an order	The Ministry of Health and Long-Term Care received a request for access to records about coverage for a procedure performed outside Canada. It was a mixed request under FIPPA and PHIPA. The Ministry provided all the FIPPA requested records (general information about the program) but refused access to some of the PHIPA health records based on proceedings and solicitor-client privilege.	The IPC ordered the Ministry to disclose one record. But upheld the Ministry's decision to withhold two other records. The IPC discussed the issue of whether certain records were "primarily dedicated to the complainant's personal health information".

	The records included email communications between Ministry staff and others.	
Decision 54 2017 Includes an order	Patient alleged her doctor disclosed more information than she agreed to when sending records to another physician relying on her express consent. The patient had subsequently sent emails changing the nature of her express consent. The patient alleged that the physician ultimately shared too much information with the recipient physician.	The IPC analyzed the "scope" of the patient's consent to disclose information to another physician and discussed what constitutes a "withdrawal" of consent to disclose. The IPC concluded that while the physician had generally responded within scope, there were a few records provided to another physician outside the scope of the patient's consent when the patient withdrew consent. The IPC ordered the physician to develop a written information practice that addresses how consents from patients to the disclosure of their PHI are to be processed, documented and clarified and to ensure that this written information practice includes a requirement for clarifying consent in situations of potential ambiguity or where there are conflicting instructions. The IPC commented generally that custodians need to be able to recreate packages of materials which are sent to other clinicians. This physician's office was able to do so.
Decision 55 2017	A chiropractor received an access request from a father for PHI of his child about a single appointment. The chiropractor provided the records. The father challenged the chiropractor's search as not being sufficiently thorough – he thought there should be additional records including for example consent for treatment records, a copy of a report provided to his former spouse and notes of telephone calls.	The IPC found the chiropractor had conducted a "reasonable search" and that there was no reason to conduct a review in this case. The IPC reiterated the test to be applied to determine a "reasonable search": 1. The custodian must provide sufficient evidence to show that it has made a reasonable effort to identify and locate responsive records. 2. A reasonable search is one in which an experienced employee knowledgeable in the subject matter of the request expends a reasonable effort to locate records which are reasonably related to the request. 3. Although a requester will rarely be in a position to indicate precisely which records the custodian has not identified, the requester must still provide a reasonable basis for concluding that such records exist.

Decision 56 2017	The Ministry of Health and Long-Term Care notified the IPC about a criminal fraud ring and concerns about the collection of health card numbers by an insurance company. The IPC was asked to review whether the insurance company should collect health card numbers for processing applications for supplementary health insurance plans (such as travel insurance and emergency medical travel insurance). The insurance company confirmed it collected health card numbers to be reimbursed for provincially insured services.	The insurance company agreed to stop collecting health card numbers as part of its application process. Instead the insurance company will collect health card numbers if there is a claim in order to be reimbursed for provincially insured services. Because the insurance company agreed to change its practices, a review by the IPC was not warranted.
Decision 57 2017	A patient made an access request at a hospital. The patient wanted to know why he was being told by physicians at the hospital to seek care somewhere else and why the chiropodist refused to see him. In particular, he wondered "what's on my medical record that is the basis for telling me to go back to the other hospital". The hospital gave the patient access to his emergency records and other visits. He believed there should be additional records. After the IPC became involved, the hospital agreed to do a further search and found there were no records of one episode and produced a copy of previously released notes. He wanted any notes, emails or letters generated during a particular time period in the Out Patient Clinic. The hospital did a further search and notified the patient that they were withholding certain records because they were not dedicated primarily to the PHI of the complainant and included PHI about others.	The IPC supported the decision of the hospital. The records related to emails between hospital staff and contained health information about the complainant. The IPC considered the test for whether a record is "dedicated primarily to the PHI of the complainant". The records were not dedicated primarily to the PHI of the patient. And there was PHI of other individuals. The hospital was right to withhold those records. The IPC considered whether the hospital completed a "reasonable search" and concluded it had.

Decision 58 2017	On behalf of herself and other siblings, a sister asked a hospital for a copy of her deceased brother's health records. The brother's death was "unexpected". The hospital declined because they were not authorized to release. After the IPC got involved, the hospital reconsidered its discretion under s. 38(4)(b) and (c) and released some records about the circumstances of death and to assist them to make decisions about their own care. The sister wanted more detailed information.	The IPC upheld the decision of the hospital. The disclosure of a deceased person's records under s. 38(4)(b) and (c) is discretionary and not mandatory. The IPC considered the meaning of "circumstances of death" and concluded that the hospital fulfilled its statutory requirements under s. 38(4)(b) and did not have to release additional information to the sister that went beyond information relating to the circumstances of death. The IPC also concluded that the hospital had fulfilled its obligations to consider its discretion under s. 38(4)(c). The sister was unable to establish that she and her siblings reasonably required the additional information to make decisions about their own care.
Decision 59 2017	A hospital received a correction request to make 5 changes to 3 Progress notes written by different clinicians. The hospital denied the correction requests stating that the entries reflected the professional opinions of its clinicians, made in good faith. The patient said the entries are a "fraud against his good character".	The IPC upheld the hospital's decision. The IPC concluded that the patient's requests reflected his desire to have the notes better explain what he was intending to communicate to the clinicians who authored the notes. But, the complainant did not establish that the records were inaccurate or incomplete for the purposes for which the hospital uses the information.
Decision 60 2017	A physician received a correction request to change two records: a 15-page patient/profile report and a 5-page subjective objective assessment plan (SOAP). The physician agreed to make 5 changes to the SOAP report reflecting typographical errors and incomplete sentences but refused to make the other changes.	The IPC upheld the physician's decision. The complainant did not establish that the records were inaccurate or incomplete for the purposes for which the physician uses the information.
Decision 61 2017	A physician received a request for access to all records relating to the complainant's deceased son. The complainant believed additional records should exist. The physician said he did not have additional records documenting contact with two other physicians – he had not spoken to the patient about these physicians and had not referred the patient to them. The complainant was looking for email communications	The IPC concluded the physician conducted a "reasonable search" and dismissed the complaint. The physician was able to describe how he reviewed his email systems and the IPC believed the physician completed the searches and found no additional records.

	between the physician and other physicians. The physician was not the deceased's primary physician. The physician had been a consultant.	
Decision 62 2017	A physician accessed health records of two related individuals without authorization in a group practice. One individual patient was deceased and the other related person was alive. The patients did not authorize the physician to view their records. It was alleged the physician then shared the information with his relative. Two corporate entities were involved. The physician was a shareholder in a medical corporation affiliated with the health centre. Both the health centre and the physician corporation were operating as health information custodians. The physician was an agent of the medical corporation. The health centre owned the electronic medical record (EMR) the physician used as part of his shareholder position.	The IPC found that the lack of documentation of the relationship between the health centre, the medical corporation and the physician caused unnecessary confusion in this case. The IPC concluded that the health centre was the health information custodian (not both the health centre and the medical corporation). The IPC focused on the fact that the health centre owned the EMR and controlled access by the physicians to the EMR and was responsible for the security of the EMR. Since the incident, the two corporations have concluded that the health centre is the health information custodian. The IPC concluded the physician used the information of the two patients without authorization. There was no information to find that the physician had disclosed the information to his relative. The IPC concluded the health centre had not met its obligations under section 12(1) at the time of the events. The group practice had since taken sufficient action so that no orders were required. The steps included: • Formalizing the relationship with the medical corporation • Ensuring all physicians were trained in privacy • Creating a joint privacy committee of both health centre members and physicians • Clarifying how discipline of physicians would be addressed in future
Decision 63 2017	A CCAC received a request to correct diagnostic or risk codes in the complainant's health record. One of the risk codes was amended, three other codes were removed from the "active" health record and a statement of disagreement was added. The CCAC was not able to "expunge" because of its duty to keep a	The IPC upheld the CCAC's decisions. The complainant was not able to prove the information held by the CCAC was inaccurate or incomplete. The IPC acknowledged the CCAC made the disputed information "inactive" and a statement of disagreement was included in the record.

	copy of any changes made to the record. Through mediation, only one issue remained for one diagnostic code relating to a diagnosis received from a referring primary care physician.	
Decision 64 2017	A hospital reported a breach involving a registration clerk accessing health records of a media-attracting patient and 443 other patients without authorization. The breach was discovered by the hospital from a proactive audit.	This file was referred to the Attorney General. The registration clerk pled guilty to contravening PHIPA and was fined $10,000. The IPC concluded that the hospital had taken sufficient steps to safeguard information specifically through: updating its privacy policies to include greater detail about the disciplinary consequences of privacy breaches; annual confidentiality agreements for all staff; privacy warning on electronic health records systems; training and sending an email to all staff re privacy and snooping; and through its auditing practices. The IPC concluded that hospitals should be able to audit the "type" of information viewed through auditing and highly encouraged the hospital to include such criteria for auditing when looking for a new electronic health record provider.

Kate Dewhirst loves privacy issues. She advises health care organizations across Ontario on anything to do with privacy. Privacy breach responses. Privacy policies. Team privacy training. Privacy Officer training. If it has to do with health privacy – she does it (and enjoys it!!).

Kate's mission is bringing the law to life. She takes legal theory and makes it understandable, accessible and fun. Kate uses storytelling to transform health care culture and make legal topics relevant and memorable. Email: kate@katedewhirst.com
Sign up for newsletters: www.katedewhirst.com Join on Facebook: Kate Dewhirst Health Law