JOHNSON SHOYAMA
GRADUATE SCHOOL OF PUBLIC POLICY
UREGINA USASK

JSGS 856 – Health Information Privacy Policy

	UNIVERSITY OF SASKATCHEWAN CAMPUS	UNIVERSITY OF REGINA CAMPUS
INSTRUCTOR:		Ramona Kyabaggu
PHONE:		Work: (306) 585-4548 Cell: 306-807-9527
E-MAIL:		ramona.kyabaggu@uregina.ca
OFFICE HOURS:		Available in person, by phone or via Zoom – all by appointment
OFFICE LOCATION:		Room 334.7, 2155 College Avenue (CB)
TERM:		Winter 2023
ROOM:		Online
DATE AND TIME:		Lectured on Fridays at 3:30 PM (Regina) unless otherwise specified

The syllabus for this course comprises this document plus the document titled "JSGS Common Syllabus 2021-22."

INTELLECTUAL PROPERTY ACKNOWLEDGEMENT

This course was developed by Ramona Kyabaggu.

CALENDAR DESCRIPTION

This course covers legislation, regulation, and standards governing access, use and disclosure of health information, ethical decision-making in information and privacy program management, and embedded privacy in the design of health infostructures. The differences between confidentiality, privacy, and security of health information are considered. Privacy, compliance, and risk policies and procedures are examined, as well as emergent data protection issues such as genomic data privacy, medical identity theft and fraud, and social media health platform privacy.

LEARNING OBJECTIVES

JSGS has developed a set of four competencies that all graduates of the MHA-HIIM will be able to demonstrate. The specific readings, assignments and activities in JSGS 856 will help you both acquire and demonstrate the ability to:

- Improve the capture, quality, and use of information to support the Canadian healthcare system.
- Understand the value, importance and influence of health information in policy, strategy and decision-making, and advance the use of information to inform and evaluate health policy and management decisions.

- Apply methods, techniques, and tools to analyze healthcare data and transform it into actionable business and clinical intelligence.
- Demonstrate cross-functional leadership and develop solutions to address the diverse needs and priorities in complex and rapidly changing healthcare systems.

COURSE CONTENT AND APPROACH

The course is taught as a combination of weekly online lecture meetings where we discuss the content for the week and allow for student Q&A. Each weekly session is recorded and shared with students who cannot attend. In-person and online office hours are available by appointment.

The content of the course spans legal, ethical, management, socio-technical and critical privacy issues from the position of the health informatician, often in juxtaposition to provider-custodians, administrators, policymakers, regulators, patients, consumers, and society at large.

The course is discussion-based. Students should do the readings to participate meaningfully in this course. Ethical decision-making cases from Harman and Cornelius' textbook and scenarios from the news media and legal courts help examine emergent privacy issues and their real-world outcomes. The intent is to strengthen the ability to interpret and make decisions as informaticians in the varied contexts that privacy activities take place.

After completing the course, students should be able to develop policies to meet - or address current gaps in - privacy legislation and make programmatic recommendations compliant with existing legal, regulatory, and standards frameworks.

REQUIRED READINGS

Harman, Laurinda B., and Cornelius, Frances H. Ethical Health Informatics: Challenges and Opportunities. Third ed. 2017. E-book available for free via the University of Regina Library (O'Reilly for Education*) at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_cdi_rittenhouse_primary_9781284053708

* Note: The O'Reilly for Education database does not offer IP authentication; you must register for an account with your uregina.ca email address.

Suggested reading material is Rozovsky, L.E., Inions, N.J., Tran, L.E. Canadian health information: A practical legal and risk management guide, 4th Edition. Location, LexisNexis, 2018. E-book and hard copy available for purchase at the UofR bookstore or through the publisher at https://store.lexisnexis.ca/en/categories/product/canadian-health-information-a-practical-legal-and-risk-management-guide-4th-edition-skusku-cad-00172/details

JOHNSON SHOYAMA

COURSE OUTLINE

Module 1 – Information Privacy Theory | Fri, Jan. 6th, 2023

This unit examines the seminal philosophical and legal theory and discourse related to identity, autonomy, information privacy, and the protection of personal information. Privacy theory in health and health care is not the main focus. The overall purpose of this module is to introduce foundational terminology, concepts, and ongoing debates in informational privacy that are relevant to health and healthcare.

Introductory forum

- Briefly introduce yourself on the introductory forum.

Forum 1 on-line discussion *due: Jan 22nd, 2023 @11:59 pm

Examples of discussion points:

1. *What is the essence of informational privacy, and how does it relate to other types of privacy within Solove's privacy taxonomy?*
2. *How can Indigenous conceptualizations of privacy be integrated into health care delivery and practice to better serve the needs of individuals and communities?*
3. *What contemporary issues have emerged that require new ways of thinking about privacy?*
4. *Are there shared, universal ideas about privacy that are not necessarily bound by time and place?*
5. *What about the notion of privacy as an inherently contested concept? Can you share an example published in the news media that juxtaposes diverging privacy discourses?*
6. *In what ways do privacy and ethics intersect? What does this relationship tell us about how health information custodians should approach privacy in their work?*
7. *Is privacy a fundamental right? Explain.*
8. *Roger Clarke presents a Maslowian perspective of privacy in which privacy of personal communication and personal data are higher-order needs that distinguish it from other types of privacy. Do you agree with this interpretation? Explain.*

Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 1 (Health Information and the Law) • 2 (Purposes of Health Information)

Required Readings:

Warren, S., Brandeis, L.D. (1890). The right to privacy. Harvard Law Review. Available at http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Clarke, R. What's 'privacy'? Roger Clarke's website: http://www.rogerclarke.com/DV/Privacy.html

Watch: https://www.youtube.com/watch?v=V5pU-8JC_PI (based on Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, Vol 79, No. 1: 119-158, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf), or listen to related podcast: https://voicesofvr.com/998-primer-on-the-contextual-integrity-theory-of-privacy-with-philosopher-helen-nissenbaum/

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154 (3): 477-564. Web.

Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_gale_legal143338178 (***Read p.477 – 483***)

Gee, K. (2019). Introduction to Indigenous Canadian Conceptions of Privacy: A Legal Primer. The Canadian Bar Association. https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2019/Runner-up-of-2019-Privacy-and-Access-Law-Student-E

Hughes, K. (2015). The social value of privacy, the value of privacy to society and human rights discourse. In B. Roessler & D. Mokrosinska (Eds.), Social Dimensions of Privacy: Interdisciplinary Perspectives (pp. 225-243). Cambridge: Cambridge University Press.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 374(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Module 2 – Information Privacy Law & Policy | Fri, Jan. 13th, 2023

This unit surveys privacy and information policy and some standards set by accrediting bodies, licensing agencies, and certification organizations. It considers the functions of Canada's court system in interpreting and setting new legal standards where no required or complete legal policy or standard exists and practical limitations therein. The Canadian Standards Association's ten fair information principles are introduced as the current framework for policy design and analysis.

Forum 2 on-line discussion (*Due: Jan 29th, 2022 @ 11:59 p.m.)

Examples of discussion points:

1. *How can government professionals, managers, and policymakers better understand information policy choices and their impacts through a purpose-driven framework lens? Consider the three primary purposes for public policy and administration information policies in your response: instrumental, value-driven, and managerial.*
2. *Describe global trends in health information policies. Is there a general agreement on principles of privacy? What can we learn from other jurisdictions?*
3. *Describe one fundamental principle outlined in the GDPR and its application to health or health care. Is there a substantially similar principle found in Canadian legislation/regulation?*
4. *What is the mandate of the Office of the Privacy Commissioner of Canada? What mechanisms are in place (or not in place) to support the Privacy Officer of Canada's enforcement of the law?*
5. *Describe some policies and procedures that health information organizations (i.e., ministries and departments of health, health agencies and authorities, health delivery organizations and research organizations) adopt for managing health information.*

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 2 (Ethical Decision-Making Guidelines and Tools)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 3 (What is Health Information) • 4 (Standards for Health Information)

Supplemental Readings:

Information Policies: Value-Oriented, Instrumental, and Managerial Choices for Governing an Information Society. In Routledge Handbook on Information Technology in Government. Available at https://www.routledgehandbooks.com/doi/10.4324/9781315683645.ch3#sec3_7_1

International Federation of Health Information. (2019). Privacy of health information, an IFHIMA Global Perspective. Available at: www.ifhima.org/whitepapers/

Office of the Privacy Commission of Canada. (2019, May). PIPEDA fair information principles. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Gillis, G. (2015). Security, privacy, and safety standards in Canadian healthcare. Journal of AHIMA 86, no.4 (April 2015): 44-46. (Uploaded to UR Courses)

Module 3 – The Legal Health Record | Fri, Jan. 20th, 2022

The module presents an overview of privacy standards for health record design, including health record documentation for legal and business purposes. We look closely at information management lifecycle approaches for paper and electronic health records and the provider-custodian role in documenting and safeguarding sensitive and personal health information. Data segmentation as an EHR- enabled the functionality to control the sharing or withholding of sensitive health record information is examined as a special topic. Standards covered are ISO/TS 14441:2013 Health informatics — security and privacy requirements of EHR systems for use in conformity assessment and HL7's International Patient Summary (IPS).

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 12 (Electronic Health Records) • One of the following chapters: 18 (Sensitive Health Information - Substance Abuse); 19 (Sensitive Health Information - Behaviour Health); 20 (Sensitive Health Information - Sexual Health)
Ethical decision-making matrices **(select one)**	• "A Curious Human Resource Employee" (Ch.13) • "EHR Integrity Management." (Ch. 15)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 5 (Retention, Storage and Disposal) • 11 (Documenting Treatment Orders) • 10 (Electronic Communications and Health Information) • 12 (Documenting Health Information) • 13 (Documenting Consent)

Supplemental Readings:

Quinsey, C.A. (2007). "Is 'legal EHR' a redundancy? Common definitions and key issues in migrating to EHRs as business records" Journal of AHIMA 78, no.2: 56-57.

Gibson, C.J., & Abrams, K.J. (2010). Will privacy concerns derail the electronic health record? Balancing the risks and benefits. In S. Kabene (Ed.), Healthcare and the effect of technology: Developments, challenges and advancements (pp. 178 -196). Hershey, PA: IGI Global. Doi:10.4018/978-1-61520-

733-6.ch011

Grando, A., Sottara, D., Singh, R., Murcko, A., Soni, H., Tang, T., Idouraine, N., Todd, M., Mote, M., Chern, D., Dye, C., & Whitfield, M. J. (2020). Pilot evaluation of sensitive data segmentation technology for privacy. International journal of medical informatics, 138, 104121. https://doi.org/10.1016/j.ijmedinf.2020.104121

Watch: Nusbaum, M. (2022). The Value of the International Patient Summary in Canada. [Webinar]. Digital Health Canada [Webinar Wednesday].

Module 4 – e-Discovery and Release of Information | Fri, Jan. 27th, 2023

This unit builds on the previous module focusing on specific stages in the lifecycle of the health record and providing a review of e-discovery and release of information (ROI) functions in health organizations. It delves into health information as evidence in legal proceedings and considerations for managing quality and handling access requests from patients, providers, payors, agencies, and institutions. The Sedona Canada Principles for Electronically Stored Information is introduced as we explore how health informaticians can support legal counsel in litigation response planning. Policy reforms to support patient rights to access their health information are also continued.

Forum 3 on-line discussion (*due: Feb 12th, 2023 @ 11:59 p.m.)

Examples of discussion points:

1. *Describe potential privacy risks during the transition from paper to electronic health records? (week 3)*
2. *Why has sensitive health information been distinguished from other types of health information? What additional factors need to be considered in handling sensitive health information?*
3. *How can the ESI principle of proportionality be met when the volume of health information collected, retained, and stored continually increases over time? Is technology-assisted review the solution?*
4. *Explain the legal argument of qualified privilege. Is there a risk that provider concerns about defamation could influence the accuracy of their documentation practice?*
5. *Should information collected using consumer technology during healthcare encounters be used as evidence?*

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Ethical decision-making matrices **(select one)**	• Chap 9: Gun Control and Reporting Mental Health Status; Conflicting Personal and Public Duties • Chap 12: Parent Access to Child's Health Information • Chap 18: Genetic Privacy • Chap 19: Seeking Information Many Years Later; An Adoptee Seeks Information on Her Biological Family; A Birth Mother Seeks Information on Her Biological Son • Chap 20: The Arrest Warrant: Is This Person in Your Facility?; Safety of a Citizen Versus Privacy of a Patient; Workers Compensation Case; Children's Protective Services; A Prisoner Who May Have AIDS (Ch. 20)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	

Chapters	• 6 (Health Information as Evidence) • 7 (Access to Health Information) • 14 (Defamation)

Supplemental Readings:

AHIMA. "Health Information Management and Litigation: How the Two Meet." Journal of AHIMA 90, no. 5 (May 2019): 38-45.

AHIMA e-Discovery Task Force. (2008). Litigation response planning and policies for E-Discovery." Journal of AHIMA 79, no.2: 69-75

CHIMA. ROI Toolkit. https://www.echima.ca/product/roi-toolkit-guide/ (free - student members)

ORDER PO-3716, Access to Information Order, Appeal PA15-558, Hamilton Health Sciences, March 31, 2017. Available at: https://decisions.ipc.on.ca/ipc-cipvp/orders/en/item/230392/index.do

El Emam, K. (2011). Physician privacy concerns when disclosing patient data for public health purposes during a pandemic influenza outbreak. BMC Public Health, 11, 1-16. Retrieved from https://bmcpublichealth.biomedcentral.com/articles/10.1186/1471-2458-11-454

Legislative Summary of Bill C-68: An Act to amend the Canadian Human Rights Act, the Privacy Act and the Personal Information Protection and Electronic Documents Act. Available at https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C68E

Krishnan, S., Shashidhar, N. (2019). eDiscovery Challenges in Healthcare. International Journal of Information Security Science. 30-43. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/2k7505/01CASLS_REGINA_ALMA5199118540003476

Verge Insurance Brokers Limited et al. v Daniel Sherk et al., 2017 ONSC 1597 (CanLII), <https://canlii.ca/t/h2mp4>, retrieved on 2022-12-31

Module 5 – Secondary Access, Use, and Disclosure of Personal Health Information | Fri, Feb. 3rd, 2023

Healthcare information management involves collecting, sharing and reporting patient data for purposes beyond direct patient care and reimbursement, including research and health policy. In recent years, healthcare digitization has enabled expanded uses of the health information collected from clinical encounters and source records—and the volume and variety of information available about patients and populations present new and unforeseen opportunities. This module is about secondary uses of health information with an emphasis on research, addressing key topics such as data linkage, data ownership, data retention and disposition, data lineage and provenance and individual consent/agency. Genomic data protection and big data open science feature as emergent areas of interest. Existing policies and resources are discussed, including the Tri-Counsel Agency Statement of Principles on Digital Data Management and Health Data Research Network Canada's new Data Access Support Hub (https://www.hdrn.ca/en/dash).

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Ethical decision-making matrices **(select one)**	• "Patient Record Integrity and Access" (Ch.12) • "Differences When Linking EHR Systems." (Ch.12)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 8: (Confidentiality, Privacy and Disclosure to Third Parties) • 9 (Digitization and Information Linkage) • 13 (Documenting Consent) • 16 (Human Research and Health Information)

Supplemental Readings:

Browse: European Health Data Space: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

Kloss, L. L., Brodnik, M. S., & Rinehart-Thompson, L. A. (2018). Access and Disclosure of Personal Health Information: A Challenging Privacy Landscape in 2016-2018. Yearbook of medical informatics, 27(1), 60–66. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_crossref10.1055/s-0038-1667071

Politou, Eugenia & Alepis, Efthymios & Patsakis, Constantinos. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions. Journal of Cybersecurity. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_oxford10.1093/cybsec/tyy001

Gliklich RE, Dreyer NA, Leavy MB, editors. Registries for Evaluating Patient Outcomes: A User's Guide [Internet]. 3rd edition. Rockville (MD): Agency for Healthcare Research and Quality (US); 2014 Apr. Available at: *https://www.ncbi.nlm.nih.gov/books/NBK208616/* **Browse only.**

Canadian Institutes of Health Research, Secondary Use of Personal Information in Health Research: Case Studies, November 2003. Retrieved from https://cihr-irsc.gc.ca/e/1475.html

Chevrier, R., Foufi, V., Gaudet-Blavignac, C., Robert, A., & Lovis, C. (2019). Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review. Journal of medical Internet research, 21(5), e13484. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_pubmed_central6658290

Boeckhout, M., Zielhuis, G. A., & Bredenoord, A. L. (2018). The FAIR guiding principles for data stewardship: fair enough? European journal of human genetics: EJHG, 26(7), 931–936. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_crossref10.1038/s41431-018-0160-0

Ploug, T., & Holm, S. (2017). Informed consent and registry-based research - the case of the Danish circumcision registry. BMC medical ethics, 18(1), 53. DOI:10.1186/s12910-017-0212-y. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_doaj_soai_doaj_org_article_5b83d09dfc8f4252a409880dacc35498

Thorogood, A. (2018). Canada: will privacy rules continue to favour open science? Human genetics, 137(8), 595–602. Available at https://pubmed.ncbi.nlm.nih.gov/30014188/

Lowrance, W. Privacy, Confidentiality, and Health Research, Cambridge University Press, 2012. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/uregina/detail.action?docID=944672.

Module 6 – Data Integrity | Fri, Feb. 10th, 2023

Privacy and protecting personal health information requires making sure that the right information is available to the right (i.e., authorized) persons at the right time and free from undue error. In this unit, we focus on the fair information principle of 'accuracy' and examine how health information's relevance, timeliness, completeness, and accuracy can impact privacy, healthcare quality, and patient safety. The importance of data quality management to identify inaccurate, incomplete and out-of-date personal health information is discussed, and methods to validate the veracity of data are considered. Contemporary issues in data processing and analysis, such as AI and algorithmic bias in health data science, are in the featured resource: Introduction to Data Ethics workbook (Vallor, 2018).

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 4 (Data Analytics)
Ethical decision-making matrices **(select one)**	• "Readmission Predictive Model Project, Part 1: Right Skills?" (Ch.4) • "Readmission Predictive Model Project, Part 2: Impact of Bad Data." (Ch.4) • "Inaccurate Publicly Reported Performance Data" (Ch.7) • "Big Data Analytics and Stewardship" (Ch.15)

Required:

Vallor, S. (2018). An Introduction to Data Ethics https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/an-introduction-to-data-ethics/

Digital Health Canada. (2021). e-Safety – Available through student membership

Supplementary Readings:

One of the following papers from the European Union Agency for Fundamental Rights:

- Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf
- #BigData: Discrimination in data-supported decision-making. Available at https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making

Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law, 20*(1), 221-256. https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_proquest2199864333

Module 7 - Privacy by Design | Fri, Feb. 17th, 2023

Malicious cybersecurity attacks are commonly reported in the news media calling for an ever-growing sophistication of strategy to stay ahead of hackers. Consistent and robust evidence indicates that the greatest threats to privacy are internal to organizations, as most data breaches result from unintended human error. In this module, we explore the nature of privacy and security incidents, violations, and

breaches and how technological, administrative, and physical safeguards can prevent breach, corruption, or loss of sensitive and personally identifiable information. Collaboration between information technology and information management professionals is discussed to enable integrated end-to-end privacy and security programs. The adoption of privacy-enhancing innovations is covered.

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 13 (Information Security)
Ethical decision-making matrices **(select one)**	• "Failure to Log Off of the System" (Ch. 13) • "Storing Data on a Laptop Computer." (Ch.13) • "Vulnerabilities in the Electronic Health Record" (Ch. 16)

Supplementary Readings:

Watch: Accenture. (2021). Improve your security posture by moving to the cloud. [Webinar]. Digital Health Canada [Webinar Wednesday].

Privacy by Design Centre of Excellence (Ryerson University). (2019 Sept 1st). Papers. Available at https://www.ryerson.ca/pbdce/papers/

Cavoukian, A., and M. Chanliau. 2013. Privacy and security by design: A convergence of paradigms. Toronto, Canada: Information and Privacy Commissioner

Inga Kroener & David Wright (2014) A Strategy for Operationalizing Privacy by Design, The Information Society, 30:5, 355-365, https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_informaworld_s10_1080_01972243_2014_944730

Nordgren, A. Privacy by Design in Personal Health Monitoring. Health Care Anal (2015) 23: 148. https://doi.org/10.1007/s10728-013-0262-3. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_springer_jour10.1007/s10728-013-0262-3

Reading Week | Monday, Feb. 20th – Saturday, Feb. 25th, 2023

There will be no classes this week.

Module 8 - Risk Management | Fri, Mar. 3rd, 2023

This module focuses on the prospective methods and tools that health information professionals can use to assess and mitigate risks, costs, and impacts to organizations of theft, corruption, and loss of personally identifiable and sensitive information. The procedural design and implementation of institutional measures for privacy program management, including privacy risk and gap assessments, privacy impact assessments and education and training, are introduced. Students are taught objective and subjective methods used for data valuation and the vital role of the organizational compliance and risk manager.

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 7 (Quality Management)
Ethical decision-making matrices **(select one)**	• "Audit Results Indicate Inappropriate Health Care" (Ch.7) • "Reporting Hospital-Acquired Conditions" (Ch.7) • "Disclosure of an Unanticipated Outcome" (Ch.7) • "Failure to Check Physician's Licensure Status." (Ch.7) • "Inconsistencies in the Patient Identity Management System." (Ch. 16)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 17: Risk Management in Health Information

Supplementary Readings:

Watch: Ooi J, Geffen I, Ahmed I. (2021). Remote Work, Data Security, and the Impact on Canadian Hospitals. [Webinar]. Digital Health Canada [Webinar Wednesday].

NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management - https://www.nist.gov/privacy-framework/privacy-framework

Module 9 – Disaster Planning and Recovery | Fri, Mar. 10th, 2023

This unit focuses on privacy and security compliance during a fire, explosion, tornado, hurricane, flood, earthquake, severe storm, power failure, bioterrorist act, or an emerging infectious disease outbreak. It emphasizes natural and human-made disasters to the exclusion of topics covered in depth in this course (e.g., cybersecurity incidences, medical identity theft and fraud). We progress through the phases of a healthcare emergency in information management (Walsh, Sheer, Roselle & Gamage, 2009), examining the administration of plans, policies, procedures and tools in five steps: risk analysis, planning and preparation, emergency activation and response, assessment and control, and business recovery. The management, safeguarding, and control of health information during major catastrophic events are emphasized (i.e., local and offsite backup types, uninterrupted power supply, redundancies, virtualization, etc.). Communication, including crisis communication, downtime documentation, and breach notification and management as a legally mandated process, are also covered, specifically the informational elements in breach notification and the importance of crisis communication to restore public confidence and trust.

Required Readings:

AHIMA. Breach Management Toolkit: A Comprehensive Guide for Compliance. Chicago, IL: AHIMA Press, April 2014.

Advancing Health Information Governance: A Global Imperative. How Data Recovery in the Wake of a Major Health Information System Failure Reinforced the Need for Information Governance. https://ifhima.files.wordpress.com/2017/10/ifhima-ig-whitepaper-final.pdf

AHIMA. (2020). Disaster Planning and Recovery Toolkit. Available at http://bok.ahima.org/PdfView?oid=302895

Brenda McPhail. (2020). Public Health, Pandemic and Privacy. Canadian Civil Liberties Association. Available at https://ccla.org/coronavirus-update-privacy/

Module 10 – Medical Identity Theft and Fraud | Fri, Mar. 17th, 2023

Medical identity theft is an increasingly common malicious criminal activity that requires specific attention in this course. We look at external threats and internal mechanisms of fraud and abuse. The ethical responsibilities of HIIM administrators to detect fraud and abuse in clinical documentation, coding, reimbursement, and reporting are addressed. Patient identity and verification processes (e.g., Accreditation Canada) are covered.

Watch: Briguglio, F. (2021). Leveraging AWS and Identity Security as the Foundation for Zero Trust in Healthcare. [Webinar]. Digital Health Canada [Webinar Wednesday].

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 5 (Compliance, Fraud and Abuse)
Ethical decision-making matrices **(select one)**	• "Documentation Does Not Justify Billed Procedure" (Ch. 5) • "Accepting Money for Information" (Ch.5) • "Retrospective Documentation to Avoid Suspension" (Ch.5) • "Coder Assigns Code Without Physician's Documentation." (Ch.5) • "Managing Patient Identification as Master Data" (Ch.15)

Module 11 – Consumer Health and Online Privacy | Fri, Mar. 24th, 2023

This module focuses on consumer health information-seeking practices. It examines the implications of trends toward personalized care, the democratization of information, and patient participation and empowerment in care decision-making enabled by the personal health record. Relevant issues are discussed, such as health and information literacy, equitable access to connected technology, and the protection of personal health data on online platforms and social media. The unit covers design principles to assess personal health records and patient portals, the Internet of Things, and the enforceability of Internet information policies such as medical advertising and anti-spam legislation.

Forum 4 online discussion due: Apr 9th, 2023 @ 11:59 p.m.

Examples of discussion points:

1. *How can design principles and policies improve consumer privacy in health application use?*
2. *Do you think the adoption of secure consumer technology will help healthcare realize the Canada Health Act's principles of public administration, accessibility, comprehensiveness, universality, and portability, or do you think consumer health technologies will undermine one or more of these principles? Explain.*
3. *Describe the digital access divide intersectionally. What equity factors might contribute to differential access and use of digital health technologies? How has inequity of access to health information and information technologies impacted individuals and populations?*
4. *Has Canada's information policy caught up to consumer technology advances? Explain.*

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Ethical decision-making matrices **(select one)**	• "Share Information on Facebook?" (Ch. 3) • "Access by Adolescents to Patient Portals." (Ch.2) • "Ensuring Privacy Protections for Digital Health Technologies." (Ch.21) • "Plain Language and Health Information Privacy Policies" (Ch. 21)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 10 (Electronic Communications and Health Information)

Supplementary Readings:

O'Loughlin, K., Neary, M., Adkins, E. C., & Schueller, S. M. (2018). Reviewing the data security and privacy policies of mobile apps for depression. Internet interventions, 15, 110–115. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_elsevier_sdoi_10_1016_j_invent_2018_12_001

Carey, R., and Burkell, J.A. (2009). "A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments." In Ian Kerr, Valerie Steeves, and Carole Lucock (Eds.) Anonymity, Identity and Privacy: Lessons from the ID Trail (pp 65-82). New York: Oxford University Press. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/2k7505/01CASLS_REGINA_ALMA51158436180003476

Cushman R, Froomkin AM, Cava A, Abril P, Goodman KW. Ethical, legal and social issues for personal health records and applications. J Biomed Inform. 2010;43(5 Suppl):S51-5. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_elsevier_sdoi_10_1016_j_jbi_2010_05_003

Essén, A., Stern, A.D., Haase, C.B. et al. Health app policy: international comparison of nine countries' approaches. npj Digit. Med. 5, 31 (2022). https://doi.org/10.1038/s41746-022-00573-1

Firano, R.F., Kushniruk, A., Barnett, J. (2017). Deriving a set of privacy specific heuristics for the assessment of PHRs (Personal Health Records). Stud Health Technol Inform; 234: 125–130. Available at https://pubmed.ncbi.nlm.nih.gov/28186028/

Househ, M., Grainger, R., Petersen, C., Bamidis, P., & Merolli, M. (2018). Balancing between privacy and patient needs for health information in the age of participatory health and social media: A Scoping Review. Yearbook of medical informatics, 27(1), 29–36. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_crossref10.1055/s-0038-1641197

Nazi K.M., Hogan T.P., Woods S.S., Simon S.R., Ralston J.D. (2016) Consumer Health Informatics: Engaging and Empowering Patients and Families. In: Finnell J., Dixon B. (eds) Clinical Informatics Study Guide. Springer, Cham. Available at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/2k7505/01CASLS_REGINA_ALMA51135411850003476

Module 13 – Issues in Critical Health Informatics | Fri, Mar. 31st, 2023

The course's final module addresses the broad social context relevant to information and privacy policy. Topics include but are not limited to the political economy of health information, ethics in public-private

data sharing, mis- and dis-information dissemination, and digital surveillance relating to the Internet of Things and mobility. We go beyond examining the literacy dimensions of privacy policies and terms of use to include critical perspectives on manufacturing consent. The rights and freedoms of individuals and populations are considered in concert with new and potentially unforeseen opportunities for digital health transformation.

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 25 (Future Challenges and Opportunities)
Ethical decision-making matrices **(select one)**	• "The Data Warehouse Wants to Sell Patient Information." (Ch. 25)

Supplemental Readings:

Diab, R., Hunt, C.DL., Neudorf, L. (2018). Privacy, Identity, and Control: Emerging Issues in Data Protection. Canadian Journal of Comparative and Contemporary Law, 4:1. Available at https://www.cjccl.ca/cjccl-2017-vol-4-1/ ***Select one article of interest to read.***

Kerr, I., Barrigar, J., Burkell, J., and Black, K. (2009). "Soft surveillance, hard consent: The law and psychology of engineering consent." In Ian Kerr, Valerie Steeves, and Carole Lucock (Eds.), Anonymity, Identity and Privacy: Lessons from the ID Trail (pp 5-22). New York: Oxford University Press. https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/2k7505/01CASLS_REGINA_ALMA51158436180003476

ASSIGNMENTS

All assessed elements are to be submitted by the stated deadlines. Online lectures follow the schedule detailed below. Each student is evaluated on the following assessed elements worth a total of 100%:

1. Four online forum discussions	**Due**	**40%**
4 x forum discussion postings	Jan 22nd, Jan 29th, Feb 12th & Apr 9th	10% each
2. One written mid-semester assignment	**Due**	**20%**
1000-word critical commentary on a topical privacy issue	Feb 19th	
3. One 2,000-word written final assignment (choose one)	**Due**	**40%**
Comparative privacy policy analysis	Apr 16th	

EVALUATION

The course is assessed via a combination of participation in online discussions, practical assignments, and a comprehensive written final report. Grades are assigned on the following basis: one mark is worth one mark towards your total mark for the course. Your final percentage is calculated as *marks achieved / total marks available*. The instructor will mark assignments according to the standards set in the Grade Descriptors for JSGS Courses, which can be found in the MHA Handbook.

Description of Assignments

Forum Discussion Participation – 40% (10% each)

Forum posts are expected on the discussion forum by 11:59 p.m. on the due date. Forum posts should provide reflection on course topics, building on in this course. Discussion prompts are provided to aid in the selection of an original post. Alternatively, students may pose their own discussion topics.

Contributions should be thoughtful with respectful consideration to the diverse ideas and viewpoints of others. Guidelines for class discussion forums are as follows:

Grading Rubric for Asynchronous Class Discussion				
Criteria	0 points	1 point	2 - 3 points	4 - 5 points
Initial posting content	No posting is made in response to the posed question. The post is inappropriate and subsequently removed by instructor.	Response attempts to answer the question but is not specific or is vague. Appears somewhat off-topic and/or does not address main point. Response late in the module week.	Response addresses the question with thought and clarity. Applies content and material from the course readings and/or lecture content in the response. Word count for initial post is between 151 and 250 words. Response by the end of the module week.	Response addresses question with thought, clarity and analysis, showing depth of understanding through application of module content: i.e., from reading material and/or lecture content. Applies concepts outside of course content, which relate to question demonstrating thoughtful analysis through use of appropriate examples. Word count for initial post is 251 words or more.
Follow-up posts	Makes 0 posts.	Makes 1 posting. Responses are one or two sentences in length. Responds late in the module week.		Responds to question and response to one, two or more classmates with thoughtful and supportive responses by the end of the module week or earlier. One or more postings include references to class content AND related content from outside sources. Response earlier in the module week.

Mid-Semester Assignment (2x) – 20%

1000-word Critical Commentary (20%):

This assignment provides the opportunity to present an analysis and critique of a substantive privacy or data protection issue relevant to health or health care that is of interest to you. Your scholarly commentary should include a position or argument rather than simply a descriptive summary on the topic.

Comprehensive Written Final Paper – 40%

This assignment requires students to evaluate a policy from a particular jurisdiction or set of jurisdictions. Students will select a provincial/territorial, national, international, or supra-national jurisdiction, outline the defining aspects of that jurisdiction's policy and present a real-world case that illustrates the current state of privacy and data protection policy in the respective jurisdiction.

The policy does not need to be a health-specific policy. Still, it should tangentially impact health or healthcare regarding privacy and data protection. Acceptable policies for analysis include legislation, regulation, directives, standards, or guidelines, in part or in full, if they are comprehensive and formally adopted by a given jurisdiction (e.g., standards formally adopted into regulation such as GDPR's privacy by design).

Students may also examine Indigenous privacy policy, respectfully sourcing information from broader knowledge sources. Subject matter should be identified by Indigenous scholars or communities as encompassing Indigenous perspectives or practices but need not be adopted into formal F/P/T policy (e.g., OCAP, UNDRIP, etc.).

General Content Guidelines	Weight
Provide a high-level introduction to your analysis, including the purpose and scope of your analysis. Present the rationale for choosing the policy from the respective jurisdiction of interest.	10%
Provide a brief description of the analytic framework or methodological lens used in your policy analysis. Outline why you selected that specific framework to analyze the policy and whether there are any important limitations for policy analysis.	10%
Analyze the relevant policy content using your preferred framework or methodological lens.	40%
Outline a real-world case example relevant to health/healthcare to substantiate your analysis, preferably one that illustrates a salient issue that emerged from your analysis. A case example could help explain policy gaps or weaknesses you identified or demonstrate how a policy has been effective. There are several sources where students can find cases (e.g., Office of the Privacy Commissioner's investigations, news media articles, court rulings from CanLII, IAPP case archives, Human Rights Watch, etc.)	20%
Briefly discuss your findings and any broad takeaways concerning the future of privacy, considering your analysis of the current state of the policy in your chosen jurisdiction.	20%
Total	**100%**

ENROLLMENT LIMIT

Class enrollment will be limited to 35 students.