JOHNSON SHOYAMA
GRADUATE SCHOOL OF PUBLIC POLICY
UREGINA USASK

JSGS 856 Health Information Privacy Policy

	UNIVERSITY OF REGINA CAMPUS
INSTRUCTOR:	Ramona Kyabaggu
PHONE:	(306) 585-4548
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:	Fall 2020
CLASSROOM(S):	Online
DATE AND TIME:	Lectured on Mondays at 7 PM (CST) unless otherwise specified

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 the design of a privacy and security infostructure. 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 issues in data protection and privacy such as genomic data privacy, medical identity theft and fraud, and social media health platform privacy.

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 meeting is recorded and shared for students who are unable to attend. In-person and online office hours are also available by appointment.

The content of the course draws on a combination of legal, ethical, management, technical, and contemporary critical privacy disciplines. This course addresses these diverse perspectives and frames the content from the position of health informatician stewards, often in juxtaposition with provider-custodians, administrators, policymakers, regulators, patients, consumers, and society-at-large.

The course format is discussion-oriented. Students should do the readings to be able to participate meaningfully in this course. A consistent theme of ethics is emphasized throughout in the form of ethical decision-making cases. The cases and further scenarios drawn from published, news media, and other sources are used to examine emergent privacy issues and their real-world outcomes. The intent is to strengthen one's ability to interpret and make decisions as specialist information consultants and administrators in the varied contexts that privacy activities take place.

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

COURSE TEXTBOOKS

Required:

Harman, Laurinda B., and Cornelius, Frances H. Ethical Health Informatics: Challenges and Opportunities. Third ed. 2017. **E-book available for free** via University of Regina Library at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/1ed24l6/TN_cdi_safari_books_9781284053708
** this database does not offer IP authentication, you will have to register for an account with your uregina.ca email address.*

Supplementary:

Rozovsky, L.E., Inions, N.J., Tran, L.E. Canadian health information: A practical legal and risk management guide, 4th Edition. Location, LexisNexus, 2018. E-book and hard copy available for purchase at https://store.lexisnexis.ca/en/categories/shop-by-jurisdiction/federal-13/canadian-health-information-a-practical-legal-and-risk-management-guide-4th-edition-skusku-cad-00172/details

COURSE OUTLINE AND ASSIGNMENTS

All assessed elements are to be submitted by 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**	**20%**
4 x forum discussion postings (5% per discussion forum)	Sep 13th & 20th, Oct 4th, Nov 23rd	
2. Two practical assignments within the semester	**Due**	**40%**
a. Design a privacy awareness training product (20%)	Oct 18th	
b. Design a privacy program - group presentation (20%)	Nov 16th	
3. One 2,500-word written final assignment (choose one)	**Due**	**40%**
a. Comparative privacy policy analysis paper	Dec 9th	
b. Critical commentary of topical privacy issue		

Module 1 – Information Privacy Theory | Sept 8th, 2020 **Rescheduled due to Labour Day*

This unit offers an examination of 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 on-going debates in informational privacy that can be applied to health.

Introductory forum

- Briefly introduce yourself and state your personal learning objectives for JSGS 856 on the introductory forum.

Forum 1 on-line discussion

Examples of discussion points:

- *What is privacy? What is the essence of informational privacy, and how does it relate to other types of privacy?*
- *How is privacy positioned within the different disciplines? For example, consider how privacy may be interpreted in Computer Sciences? Law? Business? Etc.*
- *Has the notion of privacy changed over time? What contemporary issues have emerged that require new ways of thinking about privacy?*
- *In what ways do privacy and ethics intersect? What does this relationship tell us about the roles and responsibilities of health information custodians?*
- *Should privacy be considered a fundamental right?*
- *Roger Clarke presents a Maslowian perspective of privacy in which privacy of personal communication and privacy of personal data are higher-order needs distinguished from other types of privacy. Does this hierarchal interpretation of information privacy make sense to you?*

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

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, Vol 79, No. 1: 119-158.

Watch one of the following:
https://www.youtube.com/watch?v=aVRbvxVGDoc | https://www.youtube.com/watch?v=aVRbvxVGDoc

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 the introduction p.477 – 483, and choose **one** group of activities (A. Information Collection p.491 – 503; B. Information Processing p. 504 – 522; C. Information Dissemination p. 523 – 547; or D. Invasion p. 548 - 558)*

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

Pelteret, M. & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. Informing Science: the International Journal of an Emerging Transdiscipline, 19, 277-301. Available at http://www.informingscience.org/Publications/3573

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 | Sept 14th, 2020

This unit provides a survey of comprehensive privacy and information law and policy as well as 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 10 fair information principles are introduced as a framework for policy design and analysis.

Forum 2 on-line discussion

Examples of discussion points:

- *Define the differences between instrumental, value-driven, and managerial information privacy policies and standards. Under what circumstances is it beneficial to use each of the different types of information policy?*
- *Describe global trends in health information privacy? Is there general agreement on principles of privacy? What can we learn from other jurisdictions?*
- *Outline 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? How do the federal office and it's provincial/territorial counterparts work together?*
- *How do health care organizations operationalize policies relating to the protection of information and privacy? What role do health informaticians play in creating formal support mechanisms that need to be put in place?*
- *Identify a fair information practice principle and its application to health care in Canada. What is unique about its application to the Canadian health care context?*

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	• 1 (Health Information and the Law) • 2 (Purposes of Health Information) • 3 (What is Health Information) • 4 (Standards for Health Information)

Supplemental Readings:

Young, S. (2019). Dictionary: Terms and phrases in FOIP, La FOIP & HIPA. Office of the Saskatchewan Information and Privacy Commissioner. Available at https://oipc.sk.ca/assets/dictionary.pdf

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

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

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

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

Module 3 – The Legal Health Record | Sept 21st, 2020

An overview of privacy standards for health record design, including minimum data sets and health record documentation for legal and business purposes. We look closely at information management lifecycles for governing the collection, retention, storage, and destruction of health information with a comparison of paper and electronic health record protection.

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 12 (Electronic Health Records)
Ethical decision-making matrices **(select one)**	• "EHR Integrity Management." (Ch. 15)
Canadian health information: A practical legal and risk management guide (Rozovsky & Inions, 2018)	
Chapters	• 5 (Retention, Storage and Disposal) • 12 (Documenting Health Information)

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.

AHIMA. "Fundamentals of the legal health record and designated record set." Journal of AHIMA 82, no.2: expanded online version.

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

Module 4 – e-Discovery and Release of Information | Sept 28th, 2020

This unit builds on the previous topic of the legal health record and its management and provides an in-depth analysis 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 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. Other important topics covered include the differences between privacy and confidentiality, provider-custodian accountability in safeguarding sensitive and personal health information, and patient rights to access their health information.

Forum 3 on-line discussion

Examples of discussion points:

- *Describe potential privacy risks during the transition from paper to electronic health records?*
- *What is the difference between privacy and confidentiality?*
- *Why has sensitive health information been distinguished from other types of health information? What additional factors need to be considered in the handling of sensitive health information?*
- *How might teamwork and collaboration between organizational members be necessary during the e-discovery process?*
- *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?*

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 3 (Privacy and Confidentiality) • 18 (Sensitive Health Information - Substance Abuse) • 19 (Sensitive Health Information - Behaviour Health) • 20 (Sensitive Health Information - Sexual Health)
Ethical decision-making matrices **(select one)**	• Gun Control and Reporting Mental Health Status (Ch.9) • Conflicting Personal and Public Duties (Ch.9) • Parent Access to Child's Health Information (Ch. 12) • "A Curious Human Resource Employee" (Ch.13) • Genetic Privacy (Ch. 18) • Seeking Information Many Years Later (Ch. 19) • An Adoptee Seeks Information on Her Biological Family (Ch. 19) • A Birth Mother Seeks Information on Her Biological Son (Ch. 19) • The Arrest Warrant: Is This Person in Your Facility? (Ch. 20) • Safety of a Citizen Versus Privacy of a Patient (Ch. 20) • Workers Compensation Case (Ch.20) • Children's Protective Services (Ch. 20) • 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) • 8: (Confidentiality, Privacy and Disclosure to Third Parties) • 14 (Defamation) • 15 (Employee Health Information) • Form #8 (Consent to the release of information)

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

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

El Emam, Khaled., Canadian Institute for Health Information, and Canadian Electronic Library. Practices for the Review of Data Requests and the Disclosure of Health Information by Health Ministries and Large Data. Ottawa, Ont.: CHEO Research Institute, 2011. DesLibris. Documents Collection. Web. Available at https://www.infoway-inforoute.ca/en/component/edocman/supporting-documents/498-practices-for-the-review-of-data-requests-and-the-disclosure-of-health-information-by-health-ministries-and-large-data-custodians?Itemid=101

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

Module 5 – Data Integrity | Oct 5th, 2020

Privacy and the protection of personal health information require 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 the relevance, timeliness, completeness, and overall accuracy of health information can impact privacy, health care 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 related to data processing, such as algorithmic bias in health data science, are also covered.

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)

Supplementary Readings:

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

Fernandes, L., Lenson, C., Hewitt, J., Weber, J., Yamamoto, J. (2001). Medical record number errors: A cost of doing business?

Connecting for Health Common Framework. (2006). Background issues on data quality. Available at http://bok.ahima.org/PdfView?oid=63654

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

Fernandes, L.M., O'Connor, M. "Data Governance and Data Stewardship: Critical Issues in the Move toward EHRs and HIE" Journal of AHIMA 80, no.5 (May 2009): 36-39.

AHIMA Work Group. "Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 update)" Journal of AHIMA 84, no.8 (August 2013): 58-62 [extended web version].

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 6 – Access, Use, and Disclosure of Personal Health Information | Oct 13th, 2020 *Rescheduled due to Thanksgiving

The management of health care information involves collecting and reporting data for purposes beyond direct patient care, including program management, health system administration, clinical research, and population health surveillance. In recent years, health care digitization has enabled expanded uses of the health information collected from clinical encounters and source records. Although the volume and variety of information available about patients and populations present new and unforeseen opportunities, several issues surrounding access, use, disclosure, and exchange of personal health information must be carefully examined. This module is broken down into two parts: (1) secondary uses of health information and (2) health information exchange standards.

Secondary Uses of Health Information (Part 1)

This module provides an overview of secondary data sources used in Canada and several topics related to the privacy and confidentiality of secondary personal health information in research, including consent, data ownership, and autonomy. It covers ethical frameworks governing secondary uses of health information and the responsibilities of data stewards to prevent harm to individuals. We examine technical and operational considerations for managing secondary data, including de-identification and anonymization of personal health information, linking and mining data from disparate sources, and developing a research data management plan to comply with more recent principles set out in the Tri-Counsel Agency Statement of Principles on Digital Data Management. Indigenous Data Governance, genomic data protection, and big data open science feature as emergent topics concerning significant gaps in law and policy for secondary uses.

Health Information Exchange Standards (Part 2)

This module focuses on privacy and security standards for health information exchange. We look at secure syntactic messaging and connectivity standards for interoperable health information exchange (e.g., FHIR/HL7) and policies and agreements for inter-organizational data sharing. Data segmentation as a promising strategy to control the sharing or withholding of sensitive health information is examined. Public-private data exchange and trans-border flow of personal health information are also discussed.

Assignment Due (Oct 18th, 2020) – Design a Privacy Training and Awareness Product

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	• 9 (Digitization and Information Linkage) • 13 (Documenting Consent) • 16 (Human Research and Health Information) • Form #4 (Researcher's confidentiality pledge/Confidentiality agreement) • Form #9 (Data & biological sample transfer agreement)

Supplemental Readings:

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 online book for key themes on registries as secondary sources of health information**

Canadian Institutes of Health Research, Secondary Use of Personal Information in Health Research: Case Studies, November 2002. Retrieved from http://publications.gc.ca/collections/Collection/MR21-42-2002E.pdf

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

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

Sawatsky, E. (2010). Information Sharing Agreements for Disclosure of EHR Data within Canada. http://www2.infowayinforoute.ca/Documents/ISA_report_for_HIP_Group_January_2010_EN_Final.pdf

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/

Dimick, Chris."Legal Considerations in Joining an HIE" Journal of AHIMA 82, no.10 (October 2011): 62-64.

Canadian Institute for Health Information, and Canadian Electronic Library. 'Best Practice' Guidelines for Managing the Disclosure of De-identified Health Information. Ottawa, Ont.: CHEO Research Institute, 2011. DesLibris. Documents Collection. Web. **Browse** at https://casls-primo-prod.hosted.exlibrisgroup.com/permalink/f/2k7505/01CASLS_REGINA_ALMA51133938680003476

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

Canada Health Infoway - Health Information Privacy Group (HIPG) (2012). Privacy and EHR information flows in Canada. Available at https://www.infoway-inforoute.ca/component/edocman/resources/reports/privacy/502-privacy-and-ehr-information-flows-in-canada-version-2-0?lang=en&Itemid=188

Module 7 – Privacy by Design | Oct 19th, 2020

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 strong evidence indicates that the greatest threats to privacy are internal to organizations, as most data breaches are a result of 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 to enable integrated end-to-end privacy and security programs is discussed. The adoption of privacy-enhancing innovations is covered.

Textbook Reading(s):

Ethical Health Informatics: Challenges and Opportunities (Harman & Cornelius, 2017)	
Chapters	• 13 (Information Security) • 19 (Prototype Policies and Procedures)
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:

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

Walsh, Tom. "The Proof Is in the Policy." Journal of AHIMA 75, no.2 (February 2004): 24-28.

Module 8 – Risk Management | Oct 26th, 2020

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 both objective and subjective methods used for data valuation. Policy enforcement and the vital role of the organizational compliance and risk manager is examined in depth.

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 • Form #10 (Privacy compliance checklist)

Module 9 – Incidence and Breach Notification and Response | Nov 2nd, 2020

This module provides an in-depth analysis of breach notification and management as a legally mandated process. The informational elements in breach notification and fundamentals of crisis communication to restore public confidence and trust are covered.

Required Readings:

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

Wernick, Alan S. "Connectivity, Privacy, and Liability: What Medical Professionals Must Consider" Journal of AHIMA 78, no.4 (April 2007): 64-65.

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

Module 10 – Medical Identity Theft and Fraud | Nov 16th, 2020

Medical identity theft is an increasingly common malicious criminal activity that requires specific attention in this course. We look at external threats, including data brokers involved in the monetization and transaction of personal health information. The unit goes on to explore the internal mechanisms of fraud and abuse. The ethical responsibilities and role of HIIM administrators to detect fraud and abuse in clinical documentation, coding and reimbursement, and reporting are addressed, including monitoring of retrospective documentation practices, manipulation of payment codes, and misrepresentation of resource utilization. Strategies that help detect and prevent medical identity theft and fraud, including patient identity and verification processes (e.g., Accreditation Canada), blockchain, and artificial intelligence are discussed.

Assignment Due (Nov 16th)— Designing a Privacy Management Program (Group)

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)

Supplemental Readings:

AHIMA e-HIM ™ workgroup guidelines for EPR documentation practice. Guidelines for EPR documentation to prevent fraud. Journal of AHMA, 78, no 1. (January 2007). [web extra]. – Canadian Addition: PPB #

Kulhari, S. (2018). Data Protection, Privacy and Identity: A Complex Triad. In Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity (pp. 23-37). Baden-Baden, Germany: Nomos Verlagsgesellschaft mbH. Retrieved from http://www.jstor.org/stable/j.ctv941qz6.7

Hanson, Susan P.; Cassidy, Bonnie S. "Fraud Control: New Tools, New Potential" Journal of AHIMA 77, no.3 (March 2006): 24-30.

Dougherty, Michelle. "Linking Anti-fraud and Legal EHR Functions" Journal of AHIMA 78, no.3 (March 2007): 60-61.

Module 11 – Disaster Planning and Recovery | Nov 23rd, 2020

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 health care 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, safeguard, and control of health information during major catastrophic events is emphasized; however, we spend some time on infrastructure and information technology vulnerabilities and controls, including types of local and offsite backup, uninterrupted power supply, redundancies, and virtualization. Process and functional workflow changes, communication including crisis communication, downtime documentation and communication systems, and human resource management are touched upon here. The role of the health informatics and information management professional in emergency management programs and committees is discussed.

Required Readings:

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 12 – The Personal Health Record/ Online Privacy | Nov 30th, 2020

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. Relevant issues are discussed, such as health and information literacy, equitable access to connected technology, and transparency and the protection of personal health data on online platforms and social media. The unit covers privacy heuristics to assess personal health records and patient portals, the Internet of Things, and the enforceability of Internet policies such as medical advertising and anti-spam legislation.

Forum 4 online discussion

Examples of discussion points:

- *How can heuristics be used to improve consumer privacy in human-computer interaction?*
- *How has the COVID-19 pandemic impacted digital care delivery? Do health care providers have access to the tools necessary tools to protect their patients' personal health information while delivering remote care?*
- *Will secure digital health technologies help us to realize the Canada Health Act's principles of public administration, accessibility, comprehensiveness, universality, and portability?*
- *Examine 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 technologies impacted individuals and populations?*

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

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

Module 13 – Issues in Consumer Health Informatics | Nov 8th, 2020

The final module of the course addresses the broad social context relevant to information and privacy policy. Topics include but are not be limited to the political economy of health information, privacy risks pursuant from public-private data sharing, dissemination of mis- and dis-information, and digital surveillance as it relates 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 the manufacturing of 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)

Final Assignment Due (Dec 9th)

Supplemental Readings:

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

Innovation, Science and Economic Development Canada. (May 2019). Canada's Digital Charter in Action: A Plan by Canadians, for Canadians. Available at https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

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

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*.

DESCRIPTION OF ASSIGNMENTS

Forum Discussion Participation – 20% (5% each)

Posts are expected on the discussion forum by 12 noon CST on the day before class.

Posts should provide critique and analysis on issues and build on ideas from lectures and readings in this course. Discussion prompts have been provided to aid in the selection of **one** forum posting topic as an original post. Alternatively, students may pose their own questions, share personal practice experience, where appropriate, reflect on relevant stories from the news media, or weigh-in on ethical decision-making cases of the week.

Contributions should be thoughtful with respectful consideration to the diverse ideas and viewpoints of others. Efforts made by students to post on the threads of others or respond to posts made by fellow students on their own thread will count favorably toward their participation mark 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. 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 od 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.

Practical Assignments (2x) – 40% (20% each)
Detailed assignment instructions available on UR Courses.

Comprehensive Written Final Report – 40%
Detailed assignment instructions available on UR Courses.

LATE ASSIGNMENTS

Assignments are accepted through URCourses, up to the end of the course (Dec 23rd). Any assignments that are submitted beyond the end of the course are awarded a grade of 0. It is envisaged that you can organize yourself to complete the assignments at your own pace throughout the period the course is running and are able to meet deadlines for individual assignments.

STUDENTS WITH SPECIAL NEEDS OR REQUIRING ACCOMMODATIONS

The University of Regina wishes to support all students in achieving academic success while enjoying a full and rewarding university experience.

The Centre for Student Accessibility upholds the University's commitment to a diverse and inclusive learning environment by providing services and support to enable students with disabilities, health conditions, illnesses, and injuries, to approach their studies in an equal and effective manner. The Centre for Student Accessibility aims to encourage independence, self-advocacy, and equality for all students while maintaining privacy and confidentiality.

Students who need these services are encouraged to register with the Centre for Student Accessibility to discuss the possibility of academic accommodations and other supports as early as possible. The deadline to register and/or request accommodation letters for instructors coincides with the W drop deadline for courses each semester. To register with the Centre for Student Accessibility, please book an appointment with an Accessibility Advisor by calling 306-585-4631. For further information on what is required to register and receive academic accommodation, please explore the Centre for Student Accessibility website.

STUDENTS EXPERIENCING STRESS

Students in this course who are experiencing stress can seek assistance from the University of Regina Counselling Services. For more information, please see the attached document, visit this website: http://www.uregina.ca/student/counselling/contact.html, or call (306) 585-4491 between 8:30 AM to 4:30 PM Saskatchewan time Monday to Friday.

ACADEMIC INTEGRITY AND CONDUCT

Ensuring that you understand and follow the principles of academic integrity and conduct as laid out by the University of Regina (available at https://www.uregina.ca/gradstudies/current-students/grad-calendar/policy-univ.html#conduct) is vital to your success in graduate school. Ensuring that your work is your own and reflects both your own ideas and those of others incorporated in your work is important: ensuring that you acknowledge the ideas, words, and phrases of others that you use is a vital part of the scholarly endeavour. If you have any questions at all about academic integrity in general or about specific issues, contact your course instructor to discuss your questions.