Canadian Association of Radiologists White Paper on Ethical and Legal Issues Related to Artificial Intelligence in Radiology

Jacob L. Jaremko, MD, PhD, FRCPC, Marleine Azar, MSc, Rebecca Bromwich, PhD, LLB, Andrea Lum, MD, FRCPC, Li Hsia Alicia Cheong, MDCM, Martin Gibert, PhD, François Laviolette, PhD, Bruce Gray, MD, FRCPC, Caroline Reinhold, MD, MSc, FRCPC, Mark Cicero, MD, BSc, FRCPC, Jaron Chong, MD, MHI, FRCPC, James Shaw, PhD, Frank J. Rybicki, MD, PhD, Casey Hurrell, PhD, Emil Lee, MD, FRCPC, An Tang, MD, MSc, FRCPC, for the Canadian Association of Radiologists (CAR) Artificial Intelligence Working Group

Abstract

Artificial intelligence (AI) software that analyzes medical images is becoming increasingly prevalent. Unlike earlier generations of AI software, which relied on expert knowledge to identify imaging features, machine learning approaches automatically learn to recognize these features. However, the promise of accurate personalized medicine can only be fulfilled with access to large quantities of medical data from patients. This data could be used for purposes such as predicting disease, diagnosis, treatment optimization, and prognostication. Radiology is positioned to lead development and implementation of AI algorithms and to manage the associated ethical and legal challenges. This white paper from the Canadian Association of Radiologists provides a framework for study of the legal and ethical issues related to AI in medical imaging, related to patient data (privacy, confidentiality, ownership, and sharing); algorithms (levels of autonomy, liability, and jurisprudence); practice (best practices and current legal framework); and finally, opportunities in AI from the perspective of a universal health care system.

Résumé

Les logiciels d’intelligence artificielle (IA) analysant les images médicales sont de plus en plus prévalents. Contrairement aux générations précédentes de logiciels d’IA qui reposaient sur un savoir d’expert pour identifier les caractéristiques d’une image, les approches...
Artificial intelligence (AI) and machine learning (ML) are increasingly omnipresent in modern life and becoming integrated into health care. Radiology studies are large data sets in which megabytes of image data are typically distilled into a short text-based data set (ie, the radiologist’s report) highlighting clinically relevant information (pathology or other findings termed biomarkers). AI and ML applications are highly suited to aid in this process of synthesizing key elements from raw data. Potential benefits include improved diagnostic accuracy, enhanced efficiency, new biomarker discovery, optimized post-treatment diagnosis of complications, and potentially less costly health care. Automated radiologic image diagnosis is forecast to save USD $3 billion annually in the United States “by giving radiologists more time to focus on reviews that require greater interpretation or judgment” [1].

To achieve these benefits, as observed in the Canadian Association of Radiologists’ (CAR) white paper on artificial intelligence in radiology, “AI hinges on researchers gaining access to large sets of health data from thousands of patients” [2]. Use of bulk training data allows prediction of diagnoses, prognoses, and treatment response for future patients. This shifts the relationship between patients, health care providers, and medical data [3]. Crucially, a patient’s individual data now has a new use, as part of “big data” [4]. Historically, a patient’s medical data was consulted only occasionally and solely in care of that patient, at initial consultation and follow-up, then archived and often deleted over time due to the cost of storage. With the advent of AI, ML, and personalized medicine, medical data is consulted for a new purpose: in bulk to inform the care of other patients. This secondary use of patient data imposes legal and ethical challenges related to the data, its use, and the implications of AI in radiology [2].

Data mining projects using AI to create models that can detect, diagnose, predict, and prognosticate disease processes can be seen as altruistic, on the assumption that the data sharing [5] leads to a powerful benefit to society. Tempering the incentive to share patient data for AI training is the potential threat of patient privacy and confidentiality breaches. The collection, storage, and use of bulk medical data present additional challenges related to social acceptability and public perception, legislative obstacles, information technology barriers, and the risk of breaches in data security [6].

A white paper is a “report or guide that informs readers concisely about a complex issue and presents the issuing body’s philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision” [7,8]. This white paper summarizes key ethical and legal issues pertaining to the implementation of AI and ML in radiology, primarily focusing on imaging data, although the issues raised are also pertinent to non-imaging data in electronic medical records. Issues arising from non-imaging use of AI in radiology departments, such as in optimizing workflow, are a related topic outside the scope of this paper. Although ethical principles are universal, legal and regulatory environments differ worldwide [9]. Here, we focus on a Canadian perspective. We provide a conceptual framework for further discussion and make recommendations regarding integration of AI in radiology (Table 1). Definitions are summarized in Supplemental Table 1 and abbreviations in Supplemental Table 2.

Data Value and Ownership

Access to health data has increasing commercial value, as seen with IBM’s 2015 acquisition of Merge Healthcare (USD $1 billion) that could access 5–6 million patients’ records [10]. In Canada, we are close to having a “single payer” government-funded health care system. While this could, in theory, allow access to population-wide data, the health care system remains fragmented, managed at the provincial or regional level. Access to this rich data set has great potential to enable improved health care for individual Canadians and across the Canadian population, as well as immense potential commercial value.

The issue of who owns this personal health data is characterized by a complex tension between health care provider proprietary interests, patient privacy, copyright issues, and AI developer intellectual property, and an overarching public interest in open access to data that can improve medical care. In Canada this is complicated by the constitutional division of powers, under which copyright law is in federal jurisdiction, governed by the Copyright Act R.S.C. 1985, c. C-42, while health care is in the jurisdiction of provinces and
Table 1

Key learning points

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In Canada, our public health care system provides the opportunity to develop AI decision support tools using population-wide training data, a key advantage that allows the opportunity for Canada to be a world leader in harnessing the power of AI to improve health care for its citizens.</td>
</tr>
<tr>
<td>2</td>
<td>Canadian jurisprudence reveals that the health care provider that produced a medical record owned the physical record itself and the patient has a right of access to it.</td>
</tr>
<tr>
<td>3</td>
<td>In the electronic era, the ownership of medical records and the secondary use of de-identified medical data is a complex issue that will likely depend on the type of use.</td>
</tr>
<tr>
<td>4</td>
<td>Respect of data privacy requires balancing of principles of beneficence and justice (to improve medical care for others via secondary use of an individual’s data) versus autonomy (as regards the concept of free and ongoing informed consent)</td>
</tr>
<tr>
<td>5</td>
<td>Historically, institutional review boards have granted waivers of consent when gaining explicit consent is impractical, risk associated with data sharing is minimal, and data custodian is trusted.</td>
</tr>
<tr>
<td>6</td>
<td>To facilitate development of AI applications in health care, a transition from “informed consent” for specific data uses, to “broad consent,” “opt-out consent,” and/or “presumed consent” to more general data uses is required.</td>
</tr>
<tr>
<td>7</td>
<td>Tools and policies are required to facilitate and standardize anonymization of medical images.</td>
</tr>
<tr>
<td>8</td>
<td>Public education campaigns should inform the public of the benefits that sharing of fully anonymized personal health data can provide.</td>
</tr>
<tr>
<td>9</td>
<td>Guidelines will be required prior to the deployment of AI assistive tools in hospital departments to minimize the potential harm and liability for malpractice in case of medical error involving AI.</td>
</tr>
<tr>
<td>10</td>
<td>Advances using big data and AI cause a shift in the value of data.</td>
</tr>
</tbody>
</table>

AI = artificial intelligence.

Ethical and legal issues with AI in radiology / Canadian Association of Radiologists Journal xx (2019) 1–12

In this area with relatively little Canadian legal precedent, an analogy might be made to ownership of land. Unlike in the United States, in most of Canada, a homeowner “owns” the land surface but generally not the minerals underlying their land [14] and is restricted in how they can use their land by zoning ordinances and utility rights of way. Perhaps the patient “owns” their identifiable medical data just as a landowner has surface rights, but the “mining rights” to access this data in de-identified form for purposes, such as improving health care, may be deemed to “belong” to other parties, such as the health care provider or government. In land, the meaning of “ownership” is complex and depends on the type of use it will be put to, and this is likely also true in medical data. These complex issues remain to be explored in case law as AI in health care evolves.

Data Privacy

The Constitution Act of Canada defines privacy as one of our fundamental human rights [15]. Privacy refers to an individual’s right to be free from intrusion or interference by others [16]. This right includes exercising control over information pertaining to oneself and consent for others to use that information [16]. A breach of privacy refers to the loss of, unauthorized access to, or disclosure of, personal information [17]. Personal information in radiology comprises mainly images, analogous to photos taken by various “cameras” (x-ray, ultrasound, computed tomography [CT], etc.). This data is highly personal and sensitive.

Radiology image data is particularly sensitive. Images of a person may capture something of their essence, more than words, perhaps in some ways like data contained in an individual’s own genome (which can show what gene-related conditions that individual has or risks developing). The advent of inexpensive whole-genome sequencing has led in the past 5 years to extensive consideration of issues, such as consent to secondary use of data (ie, for purposes other than an individual patient’s own medical care) [18,19]. Although medical image data is not as tightly linked to prognosis as genome data, some of the ethical issues raised are broadly similar and can inform our deliberations.

Widespread data use for AI training raises obvious concerns about data privacy, balancing on the one hand benefit and justice (improving medical care for others via secondary use of an individual’s data) versus autonomy, particularly regarding the concept of free and ongoing informed consent (Figure 1A). Privacy concerns at the level of individual patients include: how will patients know to what extent their data is undergoing secondary use; which...
portions of their data are involved; who can access their data; to what extent anonymization of data is effective and complete; whether that data could potentially be used in a way that harms them; can their data be altered; is their data being used for financial benefit of others; and will a change in data privacy policies in the near or distant future affect the care they receive.

Harm from data privacy breaches can be consequential, where a patient demonstrably suffered (eg, from discrimination, humiliation, or increased cost of insurance), or the harm can be deontological, where even if that particular patient did not suffer a negative consequence, the privacy breach still violates the duty owed by health care providers to the patient[20,21].

Concerns regarding data privacy at a societal level include: how mandatory consent may adversely affect data quality because of selection bias[22]; risks of data breaches; and how to ensure AI development leads to widespread societal benefit rather than outcomes many would not welcome, such as commoditization of personal data (data as a product).

Consent

In the setting of AI imaging analysis, a patient giving traditional consent for their data to be used may reasonably wish for information to know exactly in which models their data will be used and to whom it will be traded or transmitted, and limits on processing so that they can define how their data can and cannot be used, or even erase their data from trained models in future. Unfortunately, these wishes are challenging or even impossible to fully grant for secondary use of imaging data. Given that this secondary use is relatively new, patients will generally not have been consented for these purposes when they were imaged, leading to the current dilemma of how to handle the issue of patient consent. Historically, consent waivers have enabled researchers to access medical data for specific projects without explicit individual consent (Table 2). This waiver is typically granted by Institutional Review Boards for 2 reasons; (1) it is impractical to retrospectively obtain consent from tens or hundreds of thousands of patients, which are the sample sizes

![Diagram](image-url)

Figure 1. (A) Assuming proper respect of confidentiality and minimal risk associated with data sharing in scenarios where explicit consent is impractical, the balance between ethical principles may shift in the era of machine learning in radiology. (B) It is anticipated that the previous emphasis on fundamental rights of individuals may shift toward civic responsibility for public good.

<table>
<thead>
<tr>
<th>Exceptions to obligation for consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRBs can waive consent for secondary use research when:</td>
</tr>
<tr>
<td>1. Gaining consent is impractical.</td>
</tr>
<tr>
<td>2. Requiring consent would impair the scientific validity of the study.</td>
</tr>
<tr>
<td>3. The research addresses important health questions that pose minimal harm to participants.</td>
</tr>
</tbody>
</table>

IRB = institutional review board.
required to achieve best results in AI; and (2) the expected societal benefits of the research outweigh the perceived relatively low risk to human subjects (ie, that of a privacy breach) when appropriate protocols and data-handling measures are in place. One pathway to broader implementation of AI would be a shift from explicit consent to a new paradigm in which health care providers had more widespread default access to medical data that could be applied to AI algorithms. Beyond the potential for individual privacy breach, a risk to this expanded access is that AI may lead to broad changes in health care, and what is considered an acceptable initial risk-to-reward ratio might not be desirable after a period of time when algorithms have impacted patient care.

In the European Union, the General Data Protection Regulation deals with this by allowing patients to give a general “consent to certain areas of scientific research, when in keeping with recognized ethical standards” [23]. This type of consent has been termed “broad consent” [13] in which although the exact users of the data and exact projects are not known, the data custodian and the general parameters of possible data use are identified and agreed to. A granular “opt-out” consent system allowing certain items to be excluded is an option [24], although in many cases, this would be extremely cumbersome or logistically unmanageable to implement. “Presumed consent,” in which consent is assumed by default in settings where it would generally be considered morally wrong not to consent, is increasingly applied to posthumous organ donation [25] and could be considered for appropriately safeguarded use of health care data in AI. Consistent consent policy for AI is needed, at institutional, provincial and national levels. This will maximize the potential for collaborative innovation across borders and simplify the role of stakeholders including industry.

In Canada, the consent process is informed by the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans [16]. A 2014 amendment to this statement reads: “consent is not required for research that relies exclusively on secondary use of non-identifiable information.” This crucial change indicates that in Canada, in the opinion of the 3 main national research agencies—Canadian Institutes of Health Research, National Sciences and Engineering Research Council, and Social Sciences and Humanities Research Council—consent is not required for sharing anonymized data. Similarly, in the European Union General Data Protection Regulation, personal data can be processed without informed consent when a task is “in the public interest” [23], Article 6. This is a monumental shift in consent policy, which places increasing responsibilities on the data custodians. CAR needs to lead advocacy to ensure that this position held by Canada’s largest research agencies also makes its way to other institutions and agencies and to the general public. The optimal definition and format of a “broad consent” requires further research and consultation.

Waiver of explicit individual consent requires a guarantee of anonymity, minimal risk associated with data sharing, impracticality of explicit consent, and crucially a trusted data custodian (Figure 1B). Canadian provincial health acts vary in specific language, but in general, require removal of any data that readily identifies an individual or can be reasonably expected to be combined with other data to identify an individual [13]. The US Health Insurance Portability and Accountability Act (1996) [26] considers data to be de-identified when 18 specific data elements are absent, or if a knowledgeable expert considers there to be a “very small risk” of re-identification. Implicit in well-protected patient privacy is “data protection by design and default” [23], ie, a system where institutions and individual health care workers are structurally encouraged to work together to ensure confidentiality and security of patient data. For AI to be implemented successfully beyond individual projects, there needs to be a strong guarantee of data security and of complete anonymization of all data processed for secondary use in AI. There also needs to be a better understanding of the risks versus benefits of sharing health information.

Standardized implicit consent for appropriate secondary use of all publicly-funded health care data is crucial to enable innovation and development in AI. Government health care policies must prioritize an individual’s data privacy rights and optimize security of personal health care data over commoditization of valuable clinical data. Furthermore, there must also be public confidence that advances in AI will be implemented throughout the health care system.

The authors of this paper, representing the CAR, believe that the benefits of AI can outweigh risks when institutional protocols and technical considerations are appropriately implemented to safeguard or remove the individually identifiable components of medical imaging data. The CAR AI Working Group makes these recommendations.

**Recommendations:**

1. CAR to advocate for public education programs to increase public awareness of the benefits of sharing fully anonymized personal health data, and harm reduction strategies.
2. CAR to advocate for general adoption of revised forms of consent (such as “broad consent”) for appropriately safeguarded secondary use of data for AI in Canadian health care.
3. CAR to develop a framework to guide approaches to data security, anonymization, and secondary use of radiology data.

**Technical Aspects of Implementing Data Privacy**

The blanket approvals from institutions such as the Canadian Tri-Council and the European Union [16,23] for secondary use of non-identifiable patient data in AI presume that the data is, in fact, fully anonymized. While images of
different people can appear similar, genomic data is unique to an individual. Accordingly, the National Institutes of Health policy (for the United States) that allowed de-identified genomic data for secondary research was retracted so that since January 2015, informed consent must again be specifically given to perform unrestricted secondary research using a patient’s genetic material [27]. This is due to concerns that data can be easily re-identified from clues within the data set itself, or by combining multiple data sets [21]. In radiology data, re-identification can often be performed from inadequately processed Digital Imaging and Communications in Medicine (DICOM) image headers.

De-identification refers to removal or obscuration of personally identifying information, while anonymization refers to data that can never be re-identified, and pseudonymization refers to replacing personal identifiers with artificial identifiers [28]. Even this anonymized data remains “personal data” under European law [23,29].

Achieving true de-identification is often more challenging than expected. Radiology databases are built using DICOM files, which contain images and also meta-data within “header” fields such as “.studydate = 20140507,” “.modality = MR,” and “.PatientName = John Smith.” Anonymization requires manipulation of these file headers [30] to selectively remove or codify all identifiers. Unfortunately, each radiologic equipment manufacturer also adds their own proprietary DICOM header fields, which may contain identifying data in unexpected or un-documented locations [31]. Many picture archiving and communication systems and commercial and open-source DICOM viewer software packages offer DICOM header removal as a core feature [32,33]. One popular tool for anonymizing and transferring images is the American College of Radiology Triad package (https://triadhelp.acr.org/). Anonymization tools typically remove or replace the standard DICOM header fields but may leave proprietary fields intact, preserving personal health information [34]. Alternatively, an “additive” approach can be taken wherein a new DICOM file is constructed including image data and only a limited set of DICOM headers. The anonymization effectiveness of common software tools has been evaluated [35], but this requires reassessment with each software update. Anonymization can be (laboriously) tested by having a “white-hat” hacker attempt to find patient identifiers in sample DICOM headers. Ideally, to facilitate anonymization equipment manufacturers would not include individually identifiable information in any private or non-standard DICOM headers. CAR, along with other societies, can advocate for this change, both with manufacturers and with the custodians of the DICOM standard, the US National Electrical Manufacturers Association [36].

Anonymization can also be incomplete due to factors inherent to the imaging itself. In ultrasound or fluoroscopy, many scanners display the patient name and identification as text burned directly into the image bitmap (eg, at the top of the image). This can be obscured by image masking algorithms [35], some of which now use AI techniques [37]. For new imaging, it is often possible to have the required individually identifying data limited to a more easily removable portion of the scan, eg, only on the first image of an ultrasound or fluoroscopic study. Radiographs may also, at times, inadvertently include bracelets that allow reidentification of patients. This can be avoided through specific technologist training, or digitally masked before images are released to the picture archiving and communication system. Head/neck magnetic resonance imaging or CT scans can often be re-windowed in 3-D using a threshold calibrated to the skin surface, generating a strikingly recognizable 3-D image of the patient’s face (Figure 2) or other body parts. This image could be fed into an AI face-recognition algorithm [34]. Pre-processing with so-called “skull stripping” algorithms can help prevent this [38].

Data privacy also involves minimizing risks during the process of data transfer. Data sharing is needed between AI stakeholders, such as between a health care institution with patient data and an AI team or company performing analysis. Each method of data transfer has inherent security risks, eg, internet data interception or loss or theft of disks being physically transferred. Innovative solutions are possible where rather than bringing the data to the app, the app can be brought to the data. For example, Developer A may have an AI app they wish to try on a data set but does not want Hospital B to have access to the app code. On the other hand, Hospital B does not wish to share the data with the developer but wishes to see the results. The code from Developer A can be put into a secured container (managed by software such as Docker [39]) and allowed to run on data from Hospital B. A and B only receive the output from the code. A never sees the data, and B never sees the code, but both receive the output. This type of data sharing model is common outside health care and has potential security advantages, but is itself vulnerable to hacking and misuse [40]. This kind of model becomes impractical for very large datasets and model architectures requiring expensive hardware or the use of cloud computing.

Data privacy also requires safe storage and appropriate deletion. The principle traditionally governing data storage has been that it should be kept for no longer than is necessary for the purposes for which it was collected [21]. If data is to be stored for secondary use and is increasingly valuable as longer-term outcomes become available, a new paradigm needs to be developed.

Recommendations:

1. CAR recommends that, since DICOM de-identification/anonymization is uniquely crucial to maintaining privacy in medical imaging, a key component of any AI image analysis must be a clear protocol demonstrating how DICOM data is ensured to be truly de-identified and non-reidentifiable.

2. CAR also recommends that for any AI analysis that requires data transfer between stakeholders, a protocol be
developed specifically demonstrating the security of this transfer.

3. CAR should consider advocating to radiologists that addition of patient-identifying data to medical images that already meet DICOM standards should be standardized and easily removable in case of future anonymization.

4. CAR should consider providing links to reputable DICOM anonymization software tools.

**Role of Data Custodian: Data Sharing**

Especially when consent has not been explicitly granted for a specific project, the data custodian (such as a hospital, regional health authority, or even a radiology partnership) plays a vital gatekeeper role in determining which AI projects are ethically appropriate to perform. Authorization is usually granted by a hospital or university research ethics board, per an approved research protocol and/or data transfer agreement, could include a commercial entity with responsibility shared between parties. The legally recognized data custodian varies by institution and may be a hospital corporation with a public board of governors, or a private radiology partnership. Data custodians balance risks and benefits of data sharing by focusing on core questions: what data is being shared, who this data is being shared with, why the data is being shared, and finally, how this data is being shared. The ethical and social acceptability of usage are tied to these considerations.

The social acceptability of sharing medical data strongly depends on what data is being shared. Certain forms of data, such as the image of one’s face, psychiatric medical records, or vulnerable population status (e.g., human immunodeficiency virus status) are considered especially sensitive [41]. Other medical data can be surprisingly sensitive in certain settings, for example, a shoulder radiograph may not seem particularly private but could be sensitive if it shows pre-existing osteoarthritis that could lead to the patient being denied insurance coverage.

First, it is important to identify who data is being shared with. Researcher-to-researcher sharing commonly involves a data sharing agreement between their institutions specifying the terms under which disclosed data may be used, responsibilities in the event of data breach, permitted secondary uses (e.g., commercialization), and terms of expiry [42]. Where there is disclosure to any third-party including, but not limited to a for-profit AI company, prospective explicit *a priori* consent has traditionally been required, such as with surgical pathology biobanks [43,44]. As discussed above, emerging alternatives such as “broad consent,” “opt-out consent,” or “presumed consent” require further evaluation.

The reasons why data is shared also affect acceptability of sharing. Academic non-commercial data usage may be less controversial, with extensive precedents set [45], but there is considerable concern among the Canadian Heads of Academic Radiology regarding the ability to develop and implement academic-based algorithms that use data from within a specific medical center. Regardless of the clinical scenario and the methodology, the data custodian must decide whether and in what circumstances to grant data access to scientists, physicians, and commercial entities. It is important to recognize that many problems could arise. Although new AI routines can benefit a wide spectrum of patients, there is potential for abuse. One theoretical concern is that a company with access to hospital data in turn develops an AI routine to detect a disease without a specific, defined contractual obligation and societal commitment regarding the use and commercialization of software. If such...
assurances, contracts, and details were not in place, there would be no check on the natural tendency of a company to market and sell the routine in the interests of its shareholders rather than those of society as a whole. For example, if a company sells AI software at a high price only accessible to a small segment of the population, some might feel this violates the principle of justice.

With increasing needs to build larger models trained on more data, the technical demands of AI endeavors are influencing how data is being shared. These demands grow beyond the scope of a single hospital, clinic or radiology department to requiring specialized resources in the form of large scale graphics processing unit clusters or the use of cloud computing, the need to move data “off-site” becomes a necessity. In practice, as more and more of this data in fact lives “off-site” the notion of “on-site” and “off-site” becomes a more abstract construct implying ownership of the hardware on which the analysis is performed and, inherently, a level of supervision. While data custodians need to be mindful of this practice and ensure adequate safeguards are in place in both scenarios, whether potential benefits outweigh the added risks that an initiative requiring “off-site” analysis brings is in the hands of the Institutional Review Boards.

Data commoditization also plays a role in how much money the data is transferred for. If data is a commodity, how much is it worth? Providing data to third parties is crucial to innovation in AI. To what extent should a data custodian be able to charge for granting a third-party access to de-identified patient data? In Canada, data custodians often represent publicly funded institutions, and many of the costs to acquire, store, and maintain these records are fixed costs required for the provision of publicly-funded health care. Should the custodian be limited to recovery of costs directly related to anonymization and transfer of data, either via institutional overhead fees or on a per-record basis? How should direct costs be calculated? These will differ for dealing with medical imaging data such as large DICOM files versus other text-based clinical data. Charges exceeding direct costs provide a profit for the data custodian, which some would consider desirable, resulting in a third-party contribution that could support other aspects of health care provided by the custodian but that others would consider undesirable because high costs of data will tend to hinder innovation by stifling data access. Ideally, CAR will in the future be able to provide specific guidance on this issue to assist all stakeholders.

Relations with commercial entities risk a lack of transparency that can lead to suspicion and public backlash, as with the recent Google DeepMind/National Health Service collaboration in the United Kingdom. With the simple stated intent of developing a clinical app to identify acute kidney injury, millions of complete identifiable health records were transferred to DeepMind without patient consent, with minimal consultation of regulatory bodies, and without clear safeguards in place [46]. This was particularly controversial given that Google’s core business model involves monetizing personal data. The custodian (National Health Service) was felt by many to have placed inadequate constraints on the commercial entity, jeopardizing the privacy of millions of patients and risking data misuse. This highlights the increasingly pivotal role of the data custodian in health care AI.

The notion of intellectual property ownership rights with respect to work derived from health records is presently ambiguous. Legal analysis of previous examples have identified a complex intersection between copyright, database rights, contract laws, and personal and human rights protection [47], with greater support for data sharing when it successfully advocates for patient care improvement and innovation. Framed appropriately, the inherent asymmetries in risks to permitting regulated access to information can be balanced to maximize safe research and innovation [48].

Recommendations:

1. CAR to assist radiology data custodians by developing clear guidelines for the custodian role and preparing sample templates of data sharing agreements for common AI-related scenarios.
2. CAR to educate stakeholders on the increasing importance of the data custodian role in the absence of explicit consent.
3. CAR to work to set budgetary guidelines and formulae for departments when granting data-access to third parties.

Role of the Radiologist: Liability

Whether it is ethically appropriate to use AI depends on whether the AI will, in fact, contribute positively to individual patients and/or society. The philosopher of computer ethics JH Moor suggests that policy should be guided by the principle of “just consequentialism,” balancing considerations of justice (fairness, impartiality) with the expected positive consequences (reducing harm, increasing happiness) [49]. This is more nuanced than simply applying to AI the old, now-discarded motto of Google, “Don’t be evil.”

Just as AI in vehicles ranges from a gentle reminder that a human driver is drifting into another lane to AI completely controlling a car, AI in radiology functions at different levels of autonomy, from assisting with triage to providing a second opinion to replacing human expertise [2]. We propose a more granular classification system for levels of autonomy for AI systems applied to radiology (Table 3) based on the existing SAE International classification system for autonomous vehicles [50]. It is important to note that each modality and body system represents a separate “use case” that could be considered its own AI system. For example, level 3 autonomy for mammography may arrive before level 2 autonomy for CT head analysis. It can be argued that level 5 autonomy may never come to fruition for many use cases due to both technical and legislative considerations.
Table 3
CAR levels of autonomy for AI systems applied to radiology

<table>
<thead>
<tr>
<th>CAR level</th>
<th>Name</th>
<th>Description</th>
<th>Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No automation</td>
<td>Interpretation/intervention is done solely by the radiologist.</td>
<td>Radiologist/Clinician</td>
</tr>
<tr>
<td>1</td>
<td>Physician assistance</td>
<td>Interpretation/intervention is done primarily by the radiologist with AI providing secondary oversight (ie, existing CAD software for mammography and lung nodules, worklist prioritization).</td>
<td>Radiologist/Clinician</td>
</tr>
<tr>
<td>2</td>
<td>Partial automation</td>
<td>Interpretation/intervention is done primarily by the AI with radiologist providing secondary oversight (ie, bone age prediction, chest x-ray pathology detection and report pre-population).</td>
<td>Radiologist/Clinician</td>
</tr>
<tr>
<td>3</td>
<td>Conditional automation</td>
<td>Interpretation/intervention is done solely by the AI for a specific indication with the expectation that radiologist will intervene if the results are positive or indeterminate (ie, automated triaging of normal cases where radiologist is expected to intervene if positive but not negative).</td>
<td>AI/Radiologist/Clinician</td>
</tr>
<tr>
<td>4</td>
<td>High automation</td>
<td>Interpretation/intervention is done solely by the AI for a specific indication without the expectation that radiologist will intervene. AI is able to arrive at a differential diagnosis and recommend management autonomously (ie, AI analyzes thyroid ultrasound and recommends and/or performs biopsy for a nodule).</td>
<td>AI</td>
</tr>
<tr>
<td>5</td>
<td>Full automation</td>
<td>Interpretation/intervention is done solely by the AI for all indications expected of radiologists. AI is able to arrive at a differential diagnosis and recommend management autonomously (ie, chest x-ray requisition states “r/o pneumonia,” AI reports bone tumor with differential diagnosis and recommendations for further imaging/consultation).</td>
<td>AI</td>
</tr>
</tbody>
</table>

AI = artificial intelligence; CAD = computer-aided detection; CAR = Canadian Association of Radiologists.

In case of malpractice arising where AI was involved, it is currently unclear to what extent each involved party bears responsibility: the patient's physician, the institution at which AI was applied, the broader health care system, and/or the AI technology developer. Fear of liability can have a chilling effect; for example, discouraging data sharing out of fear that this will be used against the institution providing the data. At higher levels of AI autonomy, liability for medical errors becomes more ambiguous. The AI software may be simply non-helpful, like current computer-aided detection (CAD) software in mammography, which is ubiquitous and costly but does not necessarily improve diagnostic accuracy [51,52]. Worse, AI may be harmful. The US Food and Drug Administration states that diagnostic medical devices can be harmful in 5 ways [53]: increasing false-positive results (leading to unnecessary additional procedures), increasing false-negative results (failing to diagnose disease), being applied to inappropriate populations; being misused by human users; and malfunctioning by providing incorrect output.

AI software is viewed by regulatory bodies such as Health Canada and the Food and Drug Administration as a medical device [9]. In order to receive approval to market a device, an intended use statement must be submitted by the device manufacturer. If given approval for the intended use, the regulatory body may also place additional controls on the device to ensure safety. An example of the use case for iCAD’s Second Look Digital mammography CAD system is the following [54]:

“The MammoReader is a computer system intended to identify and mark regions of interest on standard mammographic views to bring them to the attention of the radiologist after the initial reading has been completed. Thus, the system assists the radiologist in minimizing observational oversights by identifying areas on the original mammogram that may warrant a second review.”

Based on this, relatively benign, intended-use statement, it is hard to conceive of any situation where the “AI” would be considered liable in the event of misdiagnosis. Indeed, liability with these level 1 systems continues to rest with the user (radiologist or other clinician). However, as higher levels of autonomy are intended, liability will begin to shift to the AI system and hence to the manufacturer and regulatory body. If the device is intended to autonomously diagnose a certain disease and the system is used as intended by the physician or institution, how could they be accused of malpractice? Consider a malfunctioned CT scanner exposing patients to more radiation than intended. If the institution could prove it was using the device as intended and performed appropriate maintenance, the most likely culprit for damages would be the manufacturer of the CT scanner. By this same token, damages arising from misdiagnosis by a level 4 AI system would be expected to fall on the device manufacturer. If AI interacts directly with the patient (level 5), a duty of care is formed, but if AI at the more common lower levels of autonomy only supplies a consultative opinion, eg, assists the user (radiologist or other clinician) in detecting nodules on a CT scan, it likely does not have a duty of care to the patient, which is still assumed by the clinician [55].

The institution implementing AI could potentially be held liable for AI-related medical error in several ways. It could be held responsible for malpractice under “vicarious liability” in the following circumstances: (1) if the AI system is deemed equivalent to an employee, or as a “learned intermediary,” or (2) if the AI system is deemed a technological device that the institution has a duty to deploy appropriately. The AI technology manufacturer/developer could theoretically be held liable under “products liability,” though this type of liability is notoriously difficult to demonstrate for computer software [55]. It is clear that the physician and institution are responsible to implement proper controls and use AI medical devices as intended. For example, specific
controls for iCAD’s Second Look Digital system state that the software should not be used to overturn a radiologist’s decision to call back a patient if they felt a mammogram was suspicious before using the CAD [56].

All of this remains un-tested; to date there have been no medico-legal cases at the Canadian Medical Protective Association related to AI-assisted decision-making.

Regardless of the ultimate distribution of liability in these cases, AI ought to be implemented with systemic mitigation measures in place to reduce each of the 5 risks to health from AI, providing reasonable assurance of safety and effectiveness: detailed description of algorithms, study protocols and appropriate datasets, performance testing, labelling, user training, warnings, limitations, and precautions.

Recommendations:

1. CAR to work together with other stakeholders such as provincial Ministries of Health and the Canadian Medical Protection Association to develop guidelines for appropriate deployment of AI assistive tools in hospital departments and radiology groups, seeking to minimize potential harm and institutional liability for malpractice in case of medical error involving AI.
2. Radiologists using AI should be aware of its limitations, use AI appropriately within algorithms of care, and not allow AI to replace human expert judgment.

Unmet Needs and Future Directions

Advances using “big data” such as AI and genomics have resulted in a paradigm shift in data valuation and usage (Figure 3). Older patient data has been considered to be of declining value over time as it became less relevant to that patient’s current care. These data now appear to have increasing value over time, especially when linked with longer-term longitudinal follow-up, which continuously improves the robustness and validity of the clinical outcomes to be compared with the patient’s original data at clinical presentation. For these reasons, and particularly when a commercialization component emerges, the role of the data custodian is becoming increasingly important.

In Canada, our public health care system has the opportunity to develop AI decision support tools using population-wide training data, a key advantage that could enable Canada to be a world leader in harnessing the power of AI to improve health care. In a universal health care system, positive effects of AI are more likely to be applied broadly than in a more fragmented user-pay system, in line with Moore’s principle of just consequentiality [49]. This ensures minorities are appropriately included in data sets, limiting potential bias [29]. Data sharing can be seen as a form of altruism, but this requires placing great trust in the data custodians to ensure that data is fully anonymized and is used only for appropriate purposes benefiting the public. Algorithms must be designed to function safely and as transparently as possible, minimizing a “black-box” approach. At the same time, efforts must be directed at goals maximizing health of individual patients and/or the entire population, not toward less defensible goals, such as excessive benefit to one group of patients or maximizing corporate profit [34].

Conclusions

Sharing medical data for research purposes is a complex issue balancing individual privacy rights versus potential collective societal benefits. This is particularly important for radiology AI data analysis, which uniquely requires large quantities of sensitive image data for algorithm training. A paradigm shift—from a patient’s right to near-absolute data privacy, to the sharing of anonymized data becoming regarded as one of the duties or responsibilities of a citizen—is underway. This requires a move from “informed consent” for traditional research projects, toward other forms of consent (“broad consent,” “opt-out” consent,” “presumed consent”) for AI data analyses.

Robust anonymization is crucial to AI data analyses. Best practices for anonymization in radiology can include modifications to the DICOM standard, working with manufacturers to avoid placing identifiable data in proprietary fields within DICOM files, optimizing hospital protocols to minimize data risks, encouraging researchers to use validated protocols of de-identification, and investigating safer means of data sharing such as containerization and blockchain.

Institutions (such as a hospital, health care system, or private practice group) implementing AI increasingly must act as a benevolent and enlightened data custodian. They serve as the patient’s proxy to make decisions that balance positive consequences for a particular group with justice for all groups and privacy for the individual. Especially since liability for malpractice may rest increasingly on the institution implementing AI, a radiology department or group adopting AI must pay careful attention to the algorithms integrating AI into their health care environment. As we have discussed, AI in radiology is a powerful tool with tremendous potential for individual and societal benefit and also for harm. In a world where data is increasingly valuable and the role of the data custodian is increasingly important,
implementation of AI in radiology requires thoughtful planning and frequent re-evaluation.

Acknowledgements

Fonds de recherche du Québec en Santé (FRQ-S) and Fondation de l’association des Radiologistes du Québec (FARQ) Clinical Research Scholarship Salary Award (FRQR-ARQ #34939) to An Tang.

Dr Jaremko receives unrestricted support from Medical Imaging Consultants (Edmonton) and the Alberta Health Services Chair in Diagnostic Imaging.

Disclosures

J.L.J. is one of three co-founders of MEDO.ai, a startup company investigating automated ultrasound image analysis. MEDO has no revenue, and did not provide any support for, or control over, this work. M.C. is a shareholder, co-founder, and Chief Operating Officer of 16 Bit Inc, a software company developing AI algorithms for medical image analysis. 16 Bit did not provide any support for, or control over, Dr Cicero’s contribution to this work. J.S. has received research funding from the Ontario Health Technologies Fund, VHA Home Health Care, and the Canadian Institutes of Health Research. F.J.R. is the Medical Director of Imagia Cybernetics, and the Chair of the American College of Radiology Appropriateness Criteria. None of the entities noted provided any support for, or control over, Dr Rybicki’s contribution to this work. C.H. is employed by the Canadian Association of Radiologists, which receives corporate grants from IBM Watson. E.L. is the President of the Canadian Association of Radiologists, a partial expense remunerated position, and Regional Medical Director/Regional Department Head, Department of Medical Imaging, Fraser Health Authority (FHA), BC, Canada, a contracted position with the FHA. The FHA and CAR did not provide any support for, or control over, Dr Lee’s contribution to this work. A.T. is Chair of the Canadian Association of Radiologists’ Artificial Intelligence Working Group. Dr Tang has received a research grant co-funded by MedTEQ and Imagia Cybernetics. M.A., A.L., L.H.A.C., M.G., F.L., B.G., C.R., R.B., and J.C. have no declarations of interest.

Supplementary Data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.carj.2019.03.001.

References