CMA Statement on the Governance of Health Information: A patient-partnered health information governance framework
https://policybase.cma.ca/link/policy14485

POLICY TYPE
Policy document

DATE
2022-06-29

TOPICS
Health information and e-health

WHAT IT IS
The purpose of this statement is to enhance the current health data environment and foster trust in health care delivery through the development of a patient-partnered health information governance framework. This framework will create a common standard for the management of health data and ensure that the use of health data is in the best interest of patients and health care providers. It will also establish a governance approach that ensures the protection of personal health information, respects patient autonomy, and promotes effective information use in the delivery of health care services.

1. The framework will be guided by the principles of ethical use, respect for patient autonomy, and the promotion of public health.
2. The framework will be developed through collaborative efforts among health care providers, patient representatives, and stakeholders to ensure that the health data is used in a manner that is in the best interest of patients.
3. The governance approach will be flexible and adaptable to meet the needs of different health care settings and ensure that the use of health data is in the best interest of patients.

The framework will be reviewed periodically to ensure that it remains relevant and responsive to the needs of patients and health care providers.
Guiding principles for the optimal use of data analytics by physicians at the point of care

https://policybase.cma.ca/link/policy11812

POLICY TYPE: Policy document
LAST REVIEWED: 2020-02-29
DATE: 2016-02-27
TOPICS: Health information and e-health

Documents
Principles concerning physician information
https://policybase.cma.ca/link/policy208

POLICY TYPE
Policy document

LAST REVIEWED
2019-03-03

DATE
2002-06-02

TOPICS
Health information and e-health
Ethics and medical professionalism

Documents
Guiding Principles for Physician Electronic Medical Records (EMR) Adoption in Ambulatory Clinical Practice

POLICY TYPE  
Policy document

LAST REVIEWED  
2019-03-03

DATE  
2008-02-23

TOPICS  
Health information and e-health
Vision for e-Prescribing: a joint statement by the Canadian Medical Association and the Canadian Pharmacists Association

https://policybase.cma.ca/link/policy10670

POLICY TYPE
Policy document

LAST REVIEWED
2019-03-03

DATE
2012-12-08

TOPICS
Health information and e-health
Pharmaceuticals, prescribing, cannabis, drugs

Documents
Best practices for smartphone and smart-device clinical photo taking and sharing

https://policybase.cma.ca/link/policy13860

POLICY TYPE
Policy document

DATE
2018-03-03

TOPICS
Health information and e-health
Ethics and medical professionalism

Documents

BEST PRACTICES FOR SMARTPHONE AND SMART-DEVICE CLINICAL PHOTO TAKING AND SHARING

Introduction

Clinical photography is a valuable tool for diagnosis, treatment, and follow-up care. It helps in documenting the condition, progression, and outcomes of patients. However, there are ethical and regulatory considerations that need to be addressed to ensure the safety and privacy of patients.

Best Practices

1. Obtain Informed Consent
   - Ensure that patients are informed about the purpose of taking the photograph and their rights to decline.
   - Obtain written consent if possible.

2. Respect Patient Privacy
   - Avoid identifying patients in photos.
   - Use de-identification techniques when necessary.

3. Store and Share Photos Safely
   - Use password-protected cloud storage or encrypted media.
   - Share photos only with authorized personnel.

4. Secure Data: Security and Data Protection
   - Encrypt photos and data.
   - Use strong passwords and keep them safe.

5. Legal Considerations
   - Be aware of the legal implications of using patient photos.
   - Comply with privacy laws and regulations.

6. Use Technology Wisely
   - Use technology to enhance care, not to exploit patients.
   - Avoid inappropriate use of technology.

7. Educate Patients and Staff
   - Educate patients about their rights.
   - Educate staff about best practices.

Conclusion

Clinical photography is a valuable tool, but it must be used responsibly. By following these best practices, healthcare providers can ensure the safety and privacy of patients while still benefiting from the use of technology.

Association

Canadian Medical Association

Ethics and Medical Professionalism

CMA Policybase - Canadian Medical Association
Principles for the protection of patient privacy
https://policybase.cma.ca/link/policy13833

POLICY TYPE
Policy document

DATE
2017-12-09

REPLACES
PD11-03 Principles for the Protection of Patients’ Personal Health Information

TOPICS
Health information and e-health
Ethics and medical professionalism

Documents
Guiding principles for physicians recommending mobile health applications to patients

https://policybase.cma.ca/link/policy11521

POLICY TYPE
Policy document

DATE
2015-05-30

TOPICS
Health information and e-health
Physician practice, compensation, forms

Documents

---

CMA POLICY

GUIDING PRINCIPLES FOR PHYSICIANS RECOMMENDING MOBILE HEALTH APPLICATIONS TO PATIENTS

The document is designed to provide basic information to physicians about how to use mobile health applications to improve communication about the patient's health, health care, and health information.

Three guiding principles outlined in the Canadian Medical Association's (CMA) Privacy Guidelines for the Use of Communication Technology

1. Privacy
   - Informed consent: Physicians must obtain informed consent from patients prior to recommending mobile health applications. Consent should include information about the risks and benefits of using the application, the potential for data breaches, and the patient's right to withdraw consent at any time.
   - Data protection: Personal health information should be protected according to applicable laws and regulations, such as HIPAA in the United States.
   - Anonymity: Patients' identities should be protected, and data should not be shared without their consent.

2. Security
   - Data encryption: Mobile health applications should use robust encryption techniques to protect data in transit and at rest.
   - Access controls: Access to patient data should be limited to authorized personnel.
   - Regular audits: Regular audits should be conducted to ensure compliance with security standards.

3. Trust
   - Transparency: Physicians should be transparent about the data collection and use policies of mobile health applications.
   - User-friendly design: Applications should be designed with patient privacy and security in mind.
   - Accountability: Physicians should be accountable for the use of mobile health applications and their impact on patient care.

These principles are intended to guide physicians in their recommendations of mobile health applications to patients.