Online Data Search

Status Report of available Electronic Health Data Privacy Policies:

Source	Links	Details Available Information
US Department Of Health And Human Service	http://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0ahUKEwiiouW9pZ3OAhVKsY8KHbfDA54QFghCMAU&url=http%3A%2F%2Fwww.hhs.gov%2Fsites%2Fdefault%2Ffiles%2Focr%2Fprivacy%2Fhipaa%2Funderstanding%2Fconsumers%2Fprivacy-security-electronic-records.pdf&usg=A	The Office for Civil Rights (OCR) has published new Health Insurance Portability & Accountability Act of 1996 (HIPAA) Privacy Rule guidance documents as part of a Privacy and Security Toolkit to implement The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework). These new guidance documents discuss how the Privacy Rule can facilitate the electronic exchange of health information. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearing houses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. **Keeping Your Electronic Health Information Secure** Most of us feel that our health information is private and should be protected. The federal government put in place the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to ensure you have rights over your own health information, no matter what form it is in. The Government also created the HIPAA Security Rule to require specific protections to safeguard your electronic health information. A few possible measures that can be built in to EHR systems may include: -"Access control" tools like passwords and PIN numbers, to help limit access to your information to authorized individuals. -"Encrypting" your stored information. That means your health information cannot be read or understood except by those using a system that can "decrypt" it with a "key."

	FQjCNFVKLOXP-1oeVdVrquhQAPEeJE9Pg&sig2=j4Kadzu4H5QAsG5p59GIOA&cad=rja	-An “audit trail” feature, which records who accessed your information, what changes were made and when. Finally, federal law requires doctors, hospitals, and other health care providers to notify you of a “breach.” The law also requires the health care provider to notify the Secretary of Health and Human Services. If a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. This requirement helps patients know if something has gone wrong with the protection of their information and helps keep providers accountable for EHR protection. **SHARING HEALTH INFORMATION WITH FAMILY MEMBERS AND FRIENDS** There is a federal law, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), that sets rules for health care providers and health plans about who can look at and receive your health information, including those closest to you – your family members and friends. **When Your Health Information Can be Shared?** Under HIPAA, your health care provider may share your information face-to-face, over the phone, or in writing. A health care provider or health plan may share relevant information if: You give your provider or plan permission to share the information. You are present and do not object to sharing the information. You are not present, and the provider determines based on professional judgment that it’s in your best interest. **Examples:** An emergency room doctor may discuss your treatment in front of your friend when you ask your friend to come into the treatment room. Your hospital may discuss your bill with your daughter who is with you and has a question about the charges, if you do not object. Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment. Your nurse may **not** discuss your condition with your brother if you tell her not to. HIPAA also allows health care providers to give prescription drugs, medical supplies, x-rays, and other health care items to a family member, friend, or other person you send to pick them up. A health care provider or health plan may also share relevant information if you are not around or cannot give permission when a health care provider or plan representative believes, based

		on professional judgment, that sharing the information is in your best interest.
Personal Health Information Protection Act, 2004 ONTARIO, CANADA	https://www.ontario.ca/laws/statute/04p03	Electronic protected health information (ePHI) would refer to any protected health information (PHI) that is created, stored, transmitted, or received electronically. Electronic protected health information includes any medium used to store, transmit, or receive PHI electronically. Details: Regarding Electronic Health Record here in part V.1 interpreted as "electronic health record" means the electronic systems that are developed and maintained by the prescribed organization for the purpose of enabling health information custodians to collect, use and disclose personal health information by means of the systems in accordance with this Part and the regulations made under this Part; ("dossier de santé électronique") **Requirements for electronic health record** 2. It shall not permit its employees or any other person acting on its behalf to view, handle or otherwise deal with the personal health information received from health information custodians, unless the employee or person acting on behalf of the prescribed organization agrees to comply with the restrictions that apply to the prescribed organization. 3. It shall make available to the public and to each health information custodian that provides personal health information to it, i. a plain language description of the electronic health record, including a general description of the administrative, technical and physical safeguards in place to, A. protect against theft, loss and unauthorized collection, use or disclosure of the personal health information that is accessible by means of the electronic health record, B. protect the personal health information that is accessible by means of the electronic health record against unauthorized copying, modification or disposal, and C. protect the integrity, security and confidentiality of the personal health information that is accessible by means of the electronic health record, and 4. It shall, ii. in the event that a health information custodian has requested that the prescribed organization transmit to the custodian personal health information that is accessible by means of the electronic health record, keep an electronic record of all instances where personal health information is transmitted to the custodian by means of the electronic health record, and ensure that the record identifies the individual to whom

		the information relates, the type of information that is transmitted, the custodian requesting the information, the date and time that the information was transmitted, and the location to which the information was transmitted. 5. It shall keep an electronic record of all instances where a consent directive is made, withdrawn or modified, and shall ensure that the record identifies the individual who made, withdrew or modified the consent directive, the instructions that the individual provided regarding the consent directive, the health information custodian, agent or other person to whom the directive is made, withdrawn or modified, and the date and time that the consent directive was made, withdrawn or modified. 6. It shall keep an electronic record of all instances where all or part of the personal health information that is accessible by means of the electronic health record is disclosed under section 55.7 and shall ensure that the record identifies the health information custodian that disclosed the information, the health information custodian that collected the information, any agent of the health information custodian who collected the information, the individual to whom the information relates, the type of information that was disclosed, the date and time of the disclosure and the purpose of the disclosure. 9. It shall perform, for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record, an assessment with respect to, i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and ii. how each of those systems may affect the privacy of the individuals to whom the information relates. 11. It shall notify, at the first reasonable opportunity, each health information custodian that provided personal health information to the prescribed organization if the personal health information that the health information custodian provided is stolen or lost or if it is collected, used or disclosed without authority. 13. It shall ensure that any third party it retains to assist in providing services for the purpose of developing or maintaining the electronic health record agrees to comply with the restrictions and conditions that are necessary to enable the prescribed organization to comply with all these requirements.
USA- The Health Information Privacy and Security Act of 2007 Section by	http://www.americanbar.org/content/dam/aba/migrated/health/05_health_links/News/2007/0707_	The Health Information Privacy and Security Act creates new privacy safeguards to better protect Americans' health information in the Information Age, by ensuring the right of all Americans to privacy, confidentiality and security with respect to their health information and imposing criminal and civil sanctions for the unauthorized disclosure of sensitive health information. The Security Rule is a Federal law that requires security for health information in

Section Summary	Priv_Security_Kennedy_Leahy.authcheckdam.pdf http://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/	electronic form. In this act in section 201, rules regarding use and disclosure have mentioned as • Prohibits individuals or entities from disclosing, accessing, or using protected health information without authorization. • Excepts de-identified health information from the rules in this section. • Requires that no person's protected health information be disclosed until that person has the option to opt out of any health information networks in which the receiving agent participates. • Requires that an authorized disclosure of information be the minimum amount of necessary data and be used only for the purposes for which it was authorized. • Bars unauthorized recipients of protected health information from using, accessing, or disclosing such information for any purposes. Unauthorized disclosures or use are subject to penalties established under this Act. Section 202. Authorizations for Disclosure of Protected Health Information for Treatment and Payment. Page 2 of 6 • Requires employers, health plans, health insurers, health care providers, and others seeking to disclose protected health information to obtain a signed, written authorization from an individual in connection with any treatment, payment, or other purpose. • Directs the Secretary to provide model authorization forms to assist health care providers and other persons involved in the provision of health care. • Provides that an individual may revoke or amend an authorization for protected health information concerning him at any time. • Mandates that the authorization form include: − Which information will be authorized for disclosure, who may disclose it, to whom it will be disclosed, and for what purposes; − A description of any information the individual would like segregated, generally or from a particular group; − The extent to which information will be disclosed to external systems, databases, or networks or to overseas entities; and − How authorization can be revoked. Section 203. Authorizations for Disclosure of Protected Health Information Other than for Treatment and Payment. • Requires employers, health plans, health insurers, health care providers, and others seeking to disclose protected health information for reasons other than treatment or payment to obtain a signed, written authorization from an individual that is separate from the authorization described in § 202 of this Act, and must meet only a subset of the requirements under § 202.

		• Directs the Secretary to provide model authorization forms to assist health care providers and other persons involved in the provision of health care. • Authorizes the release of protected health information to coroners and medical examiners for the purpose of inquiry into an individual's death.
Title: Security and privacy in electronic health records: A systematic literature review Journal of Biomedical Informatics Volume 46, Issue 3, June 2013, Pages 541–562 Author: **José Luis Fernández-Alemán Department Informatics and Systems, Faculty of Computer Science, University of Murcia, 30100 Murcia, Spain**	http://www.sciencedirect.com/science/article/pii/S1532046412001864	**Title: Security and privacy in electronic health records: A systematic literature review** ***Results*** A total of 49 articles were selected, of which 26 used standards or regulations related to the privacy and security of EHR data. The most widely used regulations are the Health Insurance Portability and Accountability Act (HIPAA) and the European Data Protection Directive 95/46/EC. Here found 23 articles that used symmetric key and/or asymmetric key schemes and 13 articles that employed the pseudo anonymity technique in EHR systems. A total of 11 articles propose the use of a digital signature scheme based on PKI (Public Key Infrastructure) and 13 articles propose a login/password (seven of them combined with a digital certificate or PIN) for authentication. The preferred access control model appears to be Role-Based Access Control (RBAC), since it is used in 27 studies. Ten of these studies discuss who should define the EHR systems' roles. Eleven studies discuss who should provide access to EHR data: patients or health entities. Sixteen of the articles reviewed indicate that it is necessary to override defined access policies in the case of an emergency. In 25 articles an audit-log of the system is produced. Only four studies mention that system users and/or health staff should be trained in security and privacy.
Ethical issues in electronic health	http://www.ncbi.nlm	**Title: Ethical issues in electronic health records: A general overview**

records: A general overview *-Department of Health Services, Jawahar Lal Nehru University, New Delhi, India* *-Department of Emergency Medicine, All India Institute of Medical Sciences, New Delhi, India* *-Department of Forensic Medicine, Hamdard Institute of Medical Sciences and Research, New Delhi, India*	.nih.gov/pmc/articles/PMC4394583/	Result of the study: **SECURITY BREACHES** Security breaches threaten patient privacy when confidential health information is made available to others without the individual's consent or authorization. Two recent incidents at Howard University Hospital, Washington showed that inadequate data security can affect a large number of people. On May 14, 2013, federal prosecutors charged one of the hospital's medical technicians with violating the Health Insurance Portability and Accountability Act (HIPAA). Prosecutors said that over a 17-month period, Laurie Napper used her position at the hospital to gain access to patients' names, addresses and Medicare numbers in order to sell their information. A plea hearing had been set for June 12, 2013 in which she was found guilty and sentenced for 6 months in a half-way house and fined $2,100. A few weeks earlier, the same hospital informed more than 34,000 patients that their medical data had been compromised. A contractor working with the hospital had downloaded the patient's files onto a personal laptop, which was stolen from his car. The data were password protected, but unencrypted, which means anyone who guessed the password could have accessed the patient files without a randomly generated key. By encryption, they mean encoding of information in such a way that only authorized parties can read it. It is usually done with the help of encryption key, which specifies that how the information should be decoded. According to a hospital press release, those files included names, addresses, and Social Security numbers and in a few cases, “diagnosis related information”. Recently a hospital chain named Prime Health care Services Inc. has agreed to pay $275,000 to settle a federal investigation into alleged violation of patient privacy. Keeping records secure is a challenge that doctors, public health officials and federal regulators are just beginning to understand. Cloud storage, password protection, and encryption are all measures health care providers can take to make portable EHRs more secure. A survey conducted found that 73% of physicians text other physicians about work. Mobile devices are for individual use and are not designed for centralized management by an IT Department. Mobile devices can easily be misplaced, damaged, or stolen. Emphasis must be laid on encrypting mobile devices that are used to transmit confidential information. Portable EHRs can be made more secure by using cloud storage, password protection, and encryption. Usage of two factor authentication system with security tokens and password are helpful in securing EHRs. Security measures such as firewalls, antivirus software, and intrusion detection software must be included to protect data integrity. Specific policies and procedures serve to maintain patient

		privacy and confidentiality. For example, employees must not share their ID with anyone, always log off when leaving a terminal and use their own ID to access patient digital records. A security officer must be designated by the organization to work with a team of health IT experts. Routine random audits should be conducted on a regular basis to ensure compliance with hospital policy. All system activity can be tracked by audit trails. This includes detailed listings of content, duration and the user; generating date and time for entries and logs of all modifications to EHRs. When there is inappropriate access to a medical record, the system can yield information about the name of the individual gaining access; the time, date, screens accessed and the duration of the review. This information is useful when determining whether the access is the result of an error or an intentional, unauthorized view. The HIPAA Security Rule requires organizations to conduct audit trails, requiring that they document information systems activity and have the hardware, software, and procedures to record and examine activity in systems that contain health information. Outside vendors create special privacy issues. Employee-only access to the EMR requires any external vendor to access and navigate the record under the authorization and oversight of an employee.
The Legislative Assembly Of British Columbia	https://www.leg.bc.ca/pages/bclass-legacy.aspx#/content/legacy/web/38th4th/1st_read/gov24-1.htm	**Bill 24 — 2008: E-Health (Personal Health Information Access and Protection of Privacy) Act** **Disclosure of personal health information** 5 A designation order may authorize the disclosure of personal health information only for one or more of the following purposes: (a) if disclosure is inside Canada, a purpose set out in section 4 (a) to (f) *[collection and use of personal health information]*; (b) a planning or research purpose; (c) if disclosure is inside or outside Canada, a purpose set out in section 4 (i). ***Requests for information by authorized persons*** 6 (1) A person authorized under a designation order to collect personal health information into a health information bank may request a health care body or a prescribed person to provide

		information or records that contain personal health information and that are in the custody or under the control of the health care body or prescribed person if (a) The information or records being requested have a reasonable and direct connection to the purpose for which collection is authorized under the designation order, and (b) The person making the request is acting in accordance with the terms of the designation order. (2) Subject to any other enactment that prohibits disclosure, a health care body or a prescribed person to whom a request is made under subsection (1) must comply with the request in the manner and at the times requested if the information or records are in the custody or under the control of the health care body or prescribed person. ***Effect of disclosure directives*** 10 (1) A person who is otherwise permitted to collect, use or disclose personal health information from a health information bank must not do so in any manner that is inconsistent with a disclosure directive except as follows: (a) to notify a person that a disclosure directive applies to personal health information that would otherwise be available to the person; (b) for a purpose described in section 33.1 (1) (c) of the *Freedom of Information and Protection of Privacy Act*; (c) with the express consent of the person who made the disclosure directive; (d) if section 12 *[exception — urgent or emergency health care]* of the *Health Care (Consent) and Care Facility (Admission) Act* applies and a health care provider acting under that section reasonably believes that the personal health information may be required to provide health care in accordance with that section; (e) if prescribed circumstances apply.

		(2) For the purposes of subsection (1) (d), a reference in section 12 of the *Health Care (Consent) and Care Facility (Admission) Act* to an "adult" is to be read for the purposes of this section as a reference to a person having a disclosure directive.
U.S. Department of Health and Human Services Health Information Technology	http://www.hrsa.gov/healthit/toolbox/HIVAIDSCaretoolbox/SecurityAndPrivacyIssues/howdoiensuresec.html	**How Do I Ensure Security in Our System?** Ensuring the security of protected health information (PHI) in your health IT system requires that you institute measures to guard against unauthorized use and disclosure of PHI. The HIPAA Standards for the Protection of Electronic Protected Health Information, known as the Security Rule, applies only to PHI in electronic form. As with the Privacy Rule, the Security Rule requires covered entities to have contracts or other arrangements in place with their business associates to ensure that the business associates will appropriately safeguard the electronic PHI. Below are descriptions and overviews of the administrative, physical, and technical safeguards required for the security of PHI when using electronic health IT. ***Administrative Safeguards:*** Administrative safeguards refer to the policies and procedures that exist in your practice to protect the security, privacy, and confidentiality of you patients' PHI. There are administrative safeguards that are required by both the HIPAA Privacy Rule and the HIPAA Security Rule. The administrative safeguards required under the HIPAA Security Rule include: • Identifying relevant information systems • Conducting a risk assessment • Implementing a risk management program • Acquiring IT systems and services • Creating and deploying policies and procedures • Developing and implementing a sanctions policy Assessing the risk of unauthorized use or disclosure is an important step in your overall plan for maintaining security within your system and is especially important when treating patients with HIV/AIDS. The security risk assessment and risk management safeguards are discussed further in the response to the last question of this module, "How Do I Comply with Meaningful Use Requirements?"

		Physical Safeguards: Physical safeguards for PHI and health IT refer to measures to protect the hardware and the facilities that store PHI. Physical threats, whether in electronic or paper formation, affect the security of health information. Some of the safeguards for electronic and paper-based systems are similar, but some safeguards are specific to health IT. Policies and procedures must be put in place to physically safeguard health IT. These elements include: • **Facility access controls** – Limitations for physical access to the facilities where health IT is housed, while ensuring authorized personnel are allowed access. • **Workstation use** – Specifications for the appropriate use of workstations and the characteristics of the physical environment of workstations that can access PHI. • **Workstation security** – Restrictions on access to workstations with PHI. • **Device and media controls** –Receipt and removal of hardware and electronic media that contain PHI into and out of the facility and the movement of these items within a covered entity, including disposal, reuse of media, accountability, and data backup and storage. ***Technical Safeguards:*** Technical safeguards are safeguards that are built into your health IT system to protect health information and to control access to it. This includes measures to limit access to electronic information, to encrypt and decrypt electronic information, and to guard against unauthorized access to that information while it is being transmitted to others. Procedures and policies are required to address the following elements of technical safeguards: • **Access control** - Allowing only access to persons or software programs that have appropriate access rights to data or PHI by using, for example, unique user identification protocols, emergency access procedures, automatic logoff, and encryption and decryption mechanisms. • **Audit controls** - Recording and examining activity in health IT systems that contain or use PHI. • **Integrity** - Protecting PHI from improper alteration or destruction, including implementation of mechanisms to authenticate PHI. • **Person or entity authentication** - Verifying that a person or entity seeking access to PHI is who or what they claim to be (proof of identity).

- **Transmission security** - Guarding against unauthorized access to PHI that is being transmitted over an electronic communications network.

Having technical safeguards in place can protect against various intended and unintended uses and disclosures of PHI. The table below provides examples of risks and technical safeguards. Some of these safeguards are preventive measures to protect PHI, while others ensure that you are made aware of any unauthorized uses or disclosures. Furthermore, you will need to conduct regular checks of your system so that you can see who accessed the PHI stored in your system and when it was accessed.

Risk	Technical Safeguard
PHI vulnerable to unauthorized disclosure, such as when PHI is left clearly visible on a computer screen after use	Ensure that computer locks and the screen disappears after a certain period of inactivity, and that only authorized users of that EHR can log back into the system.
PHI is exchanged with outside providers, reported to public health authorities, or moved to other media such as portable drives or a personal laptop	Ensure that all data are encrypted and transferred over secure data communication lines. Institute specific policies restricting the movement of HIV/AIDS related PHI to portable storage devices.
Health care workers, other than those who are authorized to view a patient's PHI, use the system to review the PHI to discover that patient's HIV/AIDS status	Require a password for access to PHI. Ensure that appropriate roles and role based access is defined and applied to staff. Conduct routine audit to see who has accessed sensitive data. Train all employees on the rules, regulations, and consequences of unauthorized access.
Health care workers, authorized to have access to a patient's PHI but not authorized to know the patient's HIV/AIDS status, inadvertently come across HIV/AIDS status when looking through the patient's EHR	Segregate HIV-related information into another section of the EHR that cannot be accessed unintentionally or intentionally by those without authorization. Ensure that role based access is configured and activated in the IT system. This would include any information related to HIV/AIDS status, such as test results, treatments, and participation in clinical trials or research.
Passwords are left in open areas, or	Institute a system for user authentication. Examples

passwords become vulnerable to theft from outside sources seeking to acquire patient data illegally	include using additional security codes to log in, requiring answers to a set of questions before log in, or fingerprint or iris scanning technology. Adopt a clear policy on passwords and educate staff on the policy.	

While these risks exist with both health IT and paper record systems, computer-based systems can have security features built into the software to protect against unauthorized use or disclosure. Many health IT systems have built-in security protections. Also, EHRs that are certified by ONC for Meaningful Use must meet ONC Standards and Certification Criteria. An EHR must meet nine security criteria to be certified for the first stage of Meaningful Use.

Below are the nine security protection capabilities required for EHR certification and the one optional capability. These are the minimum capabilities necessary; some EHRs will have additional security capabilities.

- Access control: permit only authorized users to access electronic health information
- Emergency access: permit authorized users to access electronic health information during an emergency
  Automatic log-off: end an electronic session after a predetermined time of inactivity
- Audit log:
  - Record actions related to electronic health information
  - Enable a user to generate an audit log for a specific time period and to sort entries
- Integrity: verify that electronic health information has not been altered in transmission and detect the alteration of audit logs
- Authentication: verify that a person seeking access to electronic health information is the one claimed and is authorized to access the information
- Encryption for general information
- Encryption when exchanging electronic health information
- Accounting of disclosures [optional]: record disclosures made for treatment, payment, and health care operations

While a certified EHR provides considerable security capabilities, you will still need to comply with the other administrative and technical safeguards to ensure the privacy and security of your patients with HIV/AIDS. In addition, you and your staff should be trained to comply with

		these protections. Online tools and resources (see Related Resources below) can be used to develop one-on-one or group training. In addition, the HITECH Act funds technical assistance and training programs to support meaningful use of EHR technologies
Title: **Legislation and Global E-Health** *Health Affairs* is the leading journal of health policy thought and research. Author: 1. *Maurice Mars (mars@ukzn.ac.za) is professor and head of the Department of Telehealth at the Nelson R. Mandela School of Medicine, University of KwaZulu-Natal, in Durban, South Africa.* *2. Richard E. Scott is a professor in the Global eHealth Research and Training Program, Department of Community Health Sciences, University of Calgary, in*	http://content.healthaffairs.org/content/29/2/237.full#ref-35	**Title: Legislation and Global E-Health** E-health law is a relatively new aspect of health for legislators. In many developed countries it is an ad hoc patchwork that focuses on only a handful of the ninety-nine e-health policy issues that have been identified.For example, Canada has some federal legislation around e-health privacy. British Columbia became the first Canadian province to create a specific legislative framework governing provincial e-health initiatives in 2008. Similarly, France has legislation for data protection, telemedicine, e-health service provision, health information technology product liability, and electronic health records. Developing or emerging nations, and some international organizations, such as the International Standards Organization, also have approved or are considering e-health policy or legislation. Malaysia's Telemedicine Act addresses the international practice of telemedicine. India has preliminary documents to address international telemedicine in an e-health act. The World Medical Association has a telemedicine policy that addresses the international practice of telemedicine. **MalaysianTelemedicine Act** Malaysia is one of the few countries with specific e-health legislation, including the Laws of Malaysia, Act 564, the Telemedicine Act of 1997. The act "provides for the regulation and control of the practice of telemedicine; and for all matters connected therewith." The Malaysian Telemedicine Act aims to protect citizens from doctors or others who might not be clinically competent. However, as written, it imposes impractical process restrictions such as requiring health care providers to register with Malaysia's Director General, a measure that can limit practices and practitioners. Also, nurses in primary health facilities must be under the "supervision of registered medical practitioners" to provide care. This means that those without access to medical practitioners may not practice telehealth. Those who breach these restrictions are subject to significant fines or imprisonment. Although well-intentioned, this legislation is an impediment to e-health. Unfortunately, as one of the few available telemedicine acts, it sets a standard that some developing-country legislators may emulate. Moreover, the Malaysian Telemedicine Act has not

Calgary, Alberta, Canada		been reviewed and updated as planned, and it no longer reflects contemporary telemedicine practice. **India** In India, policy makers are considering e-health laws that address current limits to international practice of telemedicine across borders. Options being considered are as follows: (1) mutual recognition between countries for the medical license granted by a physician's home country; (2) reciprocity between countries to allow licensed doctors to practice via e-health in both countries; (3) registration, which would ensure that physicians are liable under medical negligence and malpractice laws in the country where the e-health patient resides or communicates from; (4) limited licensure, an arrangement that allows a physician to obtain limited licensure through a licensed referring doctor in the country where the e-health patient resides or communicates from. **World Medical Association** Policies developed by this group over several years reflect the tension between ideal goals and technical limitations and reflect how e-health policy development is complex and evolving. The group's 2007 "Statement on the Ethics of Telemedicine" addresses data security: "The physician must aim to ensure that patient confidentiality and data integrity are not compromised. Data obtained during a telemedical consultation must be secured through encryption and other security precautions must be taken to prevent access by unauthorized persons." However, this language raises new questions: Do digital telephones transfer or transmit data, and what of videoconferenced teleconsultations? **E-Health Policy Development in The Developing World** A fundamental dichotomy exists between the developing and developed worlds with respect to markedly different e-health expectations and requirements. The developing world seeks ways to overcome extreme health care worker shortages and improve rural health care, at the same time improving or perhaps implementing district-level electronic health information systems. E-health policy issues in the developed world relating to data security, data quality, licensure, patient confidentiality, and privacy may be major impediments in the developing world. Indeed, developing countries are in danger of being led, unwittingly, into adopting so-called international

		best practices, which may well be inappropriate for the developing world. A natural response would be to boldly formulate new and alternative “international best practices” for the developing world. This has the danger of not just broadening the digital divide, but causing a fundamental “digital split” with developed-world and developing-world policies that may well be incompatible. A better route would be to strive for “global” e-health policy tailored to the specific needs of a given locality and population. But here, too, much remains unknown. E-health policy makers face many challenges. Using Africa as an example, there are very few people with the “global” expertise to advise African governments on e-health policy development appropriate for the continent.Politicians must weigh allocating sparse budgets to e-health and its infrastructure or to potable water, medicines, medical equipment, or health staff salaries. Given the competition for resources, perhaps it is not surprising that there are very few e-health policies or sustained e-health activities in developing countries.
Ministry of Health, Uganda, National eHealth Policy	http://library.health.go.ug/publications/leadership-and-governance-governance/policy-documents/uganda-national-ehealth-policy	To ensure security, privacy and confidentiality of Health data and information protection, Government shall: **6.5.2 Policy strategies 1** a) Develop and institutionalise the use of interoperable eHealth systems based on uniform standards and guidelines, that enable systems to interact and exchange data securely and effectively, and facilitate information sharing among users. - Develop and implement appropriate technical standards. - Develop and implement appropriate information standards. - Provide and implement a framework for the safe and secure access of health Information - Provide and implement appropriate policies and regulations.
Ministry of Health and Family Welfare, Govt. of India	http://www.nhp.gov.in/data-ownership-of-ehr_mtl	**Data Ownership of EHR** **Disclosure of information would be applicable as follows:** 1. For use for treatment, payments and other healthcare operations: In all such cases, a general consent must be taken from the patient or next of kin, etc. as defined by applicable laws. 2. Fair use for non-routine and most non-health care purposes: a specific consent must be taken from the patient; format as defined by applicable law. 3. Certain national priority activities, including notifiable/communicable diseases, will be

		specified for which health information may be disclosed to appropriate authority as mandated by law without the patient's prior authorization Responsibilities of any healthcare provider would include: 1. Protect and secure the stored health information, as per the guidelines specified in this document (chapter on Data privacy and security). 2. While providing patient information, remove patient identifying information (as provided in Table 1), if it is not necessary to be provided 3. Will ensure that there are appropriate means of informing the patient of policies relating to his/her rights to health record privacy 4. Document all its privacy policies and ensure that they are implemented and followed. This will include: 5. Develop internal privacy policies 6. Designate a privacy officer (preferably external, may be internal) who will be responsible for implementing privacy policies, audit and quality assurance 7. Provide privacy training to all its staff Patient will have the privilege to appoint a personal representative to carry out the activities detailed below. 1. Patients will have the privilege to ask for a copy of their health records held by a healthcare organization. 2. Patients will have the privilege to request a healthcare organization that holds their health records, to withhold specific information that he/she does not want disclosed to other organizations or individuals. 3. Patient can demand information from a healthcare provider on the details of disclosures performed on the patient’s health records. Instances where denial of information will apply are as follows: Healthcare provider will be able to deny information to a patient or representative or third party, in contravention of normal regulations, if in the opinion of a licensed healthcare professional the release of information would endanger the life or safety of the patients and others. This will include but not be limited to as follows: 4. Information obtained from an anonymous source under a promise of confidentiality.

		5. Psychotherapy notes. 6. Information compiled for civil, criminal or administrative action. Instances where use and disclosure without individual authorization will be possible are as follows: Disclosures can be performed without individual authorization in the following situations. • **With Identifiers**, on production of court order • However, as far as possible, and where appropriate, the data so provided should be anonymised to remove information that will allow identification of the patient. (Removing identifiers as indicated in the Patient Identifying Information Table below) **Digital signatures are to be used** to prevent non-repudiation (establishing authenticity of author of the document) and trust by the recipient.