Privacy and Security in Digital Health

(Health Data Protection Policy Sri Lanka)

Digital Health Week – 2018

12 October 2018

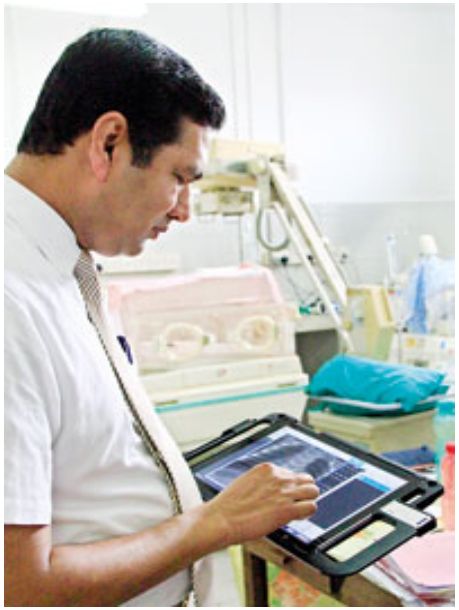
IDRC CRDI
Canada

This work was carried out with the aid of a grant from the International Development Research Centre, Canada and the Department for International Development UK

UKaid
from the British people

Why is healthcare data protection law/policy urgently required in Sri Lanka?

- Momentum is building up on greater use of ICTs within our public and private healthcare systems, particularly hospitals
- Today, data is collected, stored and processed within hospitals
  - As the data begin to move among hospitals and also to other entities within the eco system, rules will be needed
- Rules also needed with broader use of health data analytics



HHIMS Project for Health Sector
In over 50 Hospitals

HHIMS is Free and Open Source "***Hospital Health Information Management System***" specially designed for the requirement of Sri Lankan Government Hospitals. HHIMS comprises Electronic Medical Record (EMR), Computerized Provider Order Entry (CPOE), Pharmacy Management, and Laboratory Information Management and PACS integration. The system has been developed by the ICT Agency of Sri Lanka in partnership with Ministry of Health.

Data Protection – Background

- Data Protection Laws originated in Europe (Based on European Human Rights Law)
  - Right to privacy enshrined in Article 8 of EU HR Convention
  - WTO- General Agreement on Trade in Services (GATS) - Obligation to remove measures that discriminate or restrict trade in services is subject to exceptions, which include: "the protection of privacy of individuals in relation to the processing and dissemination of personal data…" (Art XIV(c)(ii))
- European Data Protection Regulations (GDPR)– May 2018
- International Trade - Relevant to Sri Lankan Companies – need to ensure same level of protection for "personal data" as in GDPR
- Legislative / Statutory approach vs. Code of Practice
- **Binding Corporate Rules – Followed by many BPM Companies**

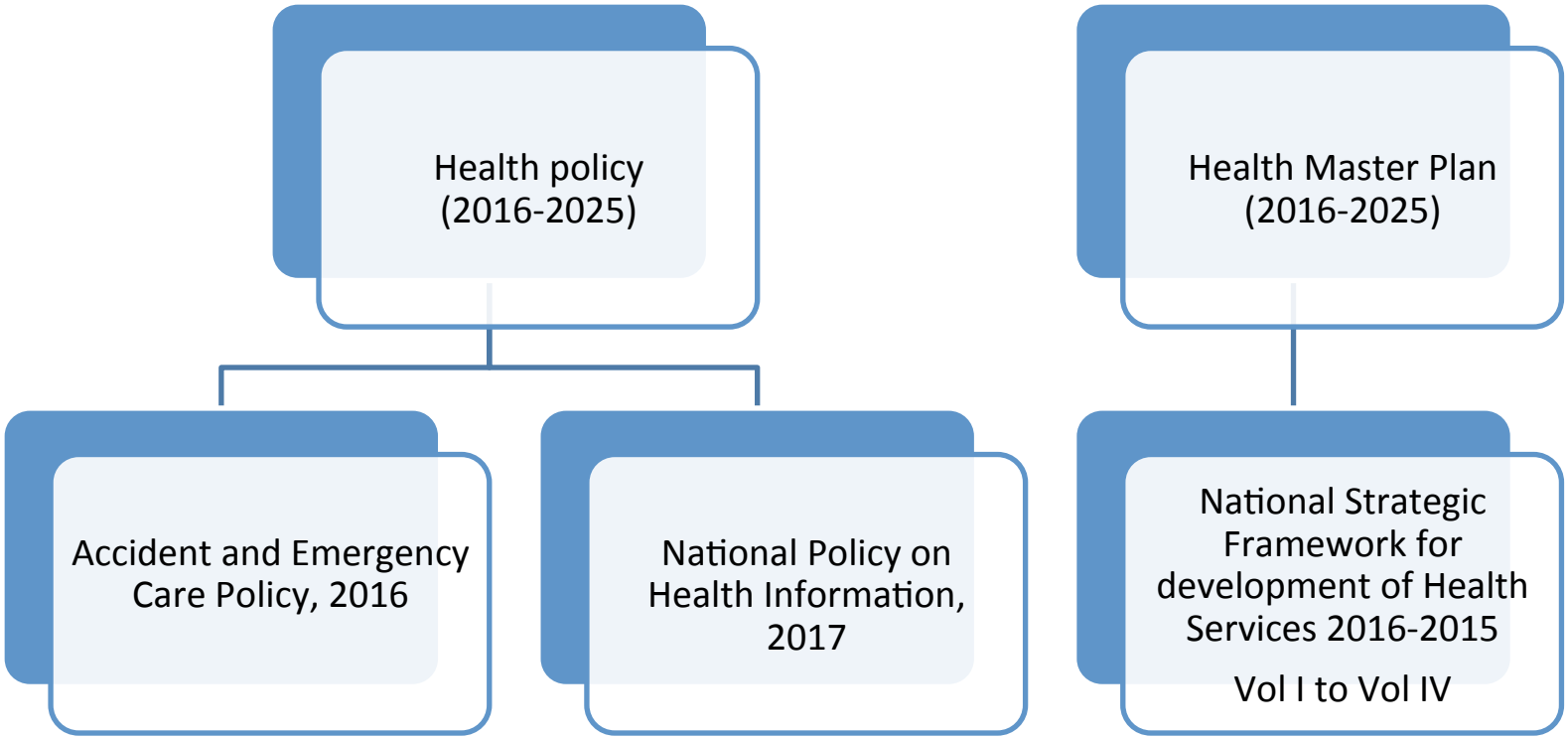
Data Protection – Sri Lanka

- No Constitutional Right to Privacy (Privacy as an Exemption)
- Right to Information Act No. 12 of 2016 (Privacy safeguards)
  - **Privacy as an exemption (Section 5)**
- Data Protection measures embodied in Several Legislation
  - Banking Act of 1988
  - Intellectual Property Act 2003 (Protection of undisclosed information)
  - Computer Crimes Act of 2007 (Mechanism to report Data Breach)
  - Registration of Persons (Amendment) Act No. 8 of 2016 (Regulations 2017)
- E-Government Policy (Section 0103)
  - Processing/ Retention/ release of personal data and information in accordance with applicable laws and regulations
  - Email addresses of citizens collected through govt websites should not be divulged

Health Data Protection – at a Glance

Jurisdiction	Summary of overall approach
EU-GDPR	• Comprehensive data protection framework (that includes healthcare data) • Rights based approach- individual at center of law • Applies to processing of personal data and covers both private sector as well as government
USA	• Sectoral data protection framework; HIPAA for healthcare • Approaches different for private sector and government
Australia	• Similar to the US framework • Approaches different for private sector and government
UK	• Amended data protection legislation in line with GDPR
India	• Currently healthcare data is classified as 'sensitive personal data' • Governed under Information Technology (Reasonable Security Practices And Procedures and Sensitive Personal Data or Information Rules (2011); specifically under Sensitive Personal Data or Information (SPDI Rules) • A new comprehensive data protection bill drafted in 2018, draft bill has been published, but has not yet been adopted
Singapore	• General data protection legislation; advisory guidelines for health sector

Relevant recently adopted policies in Sri Lanka



In addition:

- National Health Performance Framework, 2018
- Code of Conduct for Health Research in Sri Lanka, 2018
- National Health Development Plan (2013-2017)
- National eHealth Guidelines and Standards V 1.0 (2016)

National Policy on Health Information 2017

Lays down directives in relation to 5 areas :

A. Health information related resources
B. Indicators and data elements
C. Data and Information management
D. Data / information security, client privacy, confidentiality and ethics
E. e- health and innovations

National Policy on Health Information 2017

Some important policy directives include:

- Establishment of a body for e-health and governance
  - National eHealth Steering Committee [NeHSC]
- Provisions for
  - Implementation of Health Information System (HIS)
  - Interoperability of HIS -Policy Directive 5.3
  - Longitudinal record of health data –Policy Directive 3.2
  -Unique Patient ID - Policy Directive 3.2.1, personal health number (PHN) assigned for all health clients
  - Integration of data - Policy Directive 2.2, information integration between State and Non- State actors

Health Data Protection in Sri Lanka

- The national Policy on Health Information, states that "*Ethical and fair information practices shall be incorporated into information management ensuring client privacy and confidentiality*"- Policy Directive 4.1

- The Health Information Policy states *guidelines are needed for the collection of individually identifiable data/ information to possess qualities of relevance, integrity, a written purpose, the capacity for correction and consent of the individual (the responsibility for the same has also been allocated).*

Aim of Health Data Protection Policy

- To protect patient- identifiable information
- To facilitate the use of health data in medical research so as to enhance individual and public health
- To provide for use of health data and the applicable safeguards for such use.

Issues

- Scope of “health data”
- Defining data protection obligations
- Defining electronic health records
- Use of data (exceptions) and safeguards
- Regulatory / supervisory authority

SCOPE OF REGULATION

Proposed Framework

- Since Sri Lanka does not yet have general data protection legislation, the scope should be narrowly defined
  - "Health record/information" can be defined broadly. However, the application of the policy may be restricted to entities providing health service (example the legislation in UK, US and Australia) or who come into possession of such health information in the course of their primary business (e.g., insurance companies, as included under the US HIPAA Act)
  - instead of an exhaustive list provision would be made for further inclusions. For example the Australia Privacy Act provides examples of "health service providers" and not an exhaustive list
- Inclusion of healthcare data processed and /or transferred outside of Sri Lanka would also be considered

DATA PROTECTION OBLIGATIONS

Regulation in other jurisdictions

Jurisdiction	Summary of regulation
EU-GDPR	• Health data (considered as sensitive data) cannot be processed unless explicit consent has been obtained, or presence of other overriding considerations like public interest, scientific research etc.
India	• The Draft Personal Data Protection Bill, 2018 encompasses in great detail the data protection principles. Classifies “health data” as sensitive personal data. • The DISHA (Draft legislation) deals with data ownership, security and standardization.
Australia	• Health data is classified as “sensitive” • The Australia Privacy Principles lay down the data protection obligations.
UK	• There is a general data protection law in addition to health data specific privacy principles.
US	• The Privacy Rule of the HIPPA provides for protection of protected health information.
Singapore	• General data protection legislation; issued advisory guidelines for the health sector

Personally identifiable data

- Distinction has to be made between health data where personal information is identifiable and where they are not (anonymized / de-identified).
- The principles of confidentiality, consent and other data protection obligations are applicable to health data which are “personally identifiable.”
- Personal data has been subject to various definitions in analyzed jurisdictions-

Informed Consent

- In relation to *consent* the proposed policy would, *inter alia* include: (partially adopted from the Singapore Personal Data Protection Act and India)
  - Disclosure of purpose for obtaining the consent
  - Consent has to be untilised for that purpose and not for other purpose
  - Consent may be provided for several purposes provided the terms clearly specify the same.
  - The consent should be clear, evidenced through affirmative action (opt-in as opposed to opt-out)
  - Such consent should be capable of being withdrawn.
  - Deemed consent –under limited circumstances.
  - Consent forms should be provided in clear and simple language and made available in all the official languages

Other pertinent considerations

- Data Controller and Processor
- The measures required to ensure information security.
  - The *Information Security Policy Domains by SL- CERT* is of relevance in this regard
- Consent from children and those who are incapacitated to provide consent
- Data of dead persons
- Cross-border transfer of data

Summary - Principles of Data Protection

The proposed policy will focus on the following principles to build the data protection framework :

- *Technology agnosticism* (technology neutral to take into account changing technologies and standards of compliance)
- Application to both *private* and *public* heath sectors
- *Informed consent*
- *Data minimization* (processing of only data that is required for the purpose)
- *Controller accountability* (making the data controller accountable for any processing of data)
- Framing of subsequent regulations to *ensure compliance*.

USE OF DATA (EXCEPTIONS) & SAFEGUARDS

Use and Safeguards

Jurisdiction	Summary of schemes
UK	• Mandatory disclosure • Incorporated the provisions of the GDPR • Code for anonymization
Australia	• Disclosure of personal information without consent • Framework for de-identification
India	• DISHA Act (draft for consultation) provides for de-identification – anonymization
US	• Disclosure of personal information without consent • De-identification through safe harbor or expert determination
Singapore	• Disclosure without obtaining consent • Advisory guidelines for anonymization of data.
GDPR	• Disclosure without obtaining consent provided the safeguards are met • Use of personal data for scientific research, *qualified compliance framework*.

Proposed Framework

- In the proposed policy this section would include three parts
  - Permitting Disclosure when information is not personally identifiable .
  - Anonymization / de-identification to ensure personal information is not re-identified
  - Mandatory disclosure / exceptional instances where even information that is personally identifiable would need to be disclosed.
- This section aims at striking a balance between protection and necessary disclosure.

Mandatory Disclosures (UK)

- *The Health and Social Care (Safety and Quality) Act 2015* introduced a legal duty for health and social care professionals to share patient information where they consider that the disclosure is likely to facilitate patient care and is in the patient's best interest.
- *Health Protection (Notification) Regulations 2010* – a health professional must notify local authorities about any person suspected of having a range of listed conditions, including food poisoning, measles and tetanus.
- *Abortion Regulations 1991* – a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving the individual's date of birth and postcode.
- *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013* – deaths, major injuries and accidents resulting in three days off work, as well as certain diseases and dangerous occurrences, must be reported.

Anonymization of data

UK

- The GDPR principles have been incorporated in the UK.
- The Code of Anonymization provides a standard for anonymization of data sets. Note this Code is under the 1998 legislation
- Disclosure of such anonymized data would not be subject to the data protection legislation, providing an incentive for organizations and researchers to anonymize data.

Disclosure without consent (US)

- HIPAA “covered entities” are permitted to use and disclose Protected Health information (PHI) without the individual’s authorization in certain situations. For example,
- Between business associates
- For public health purposes as required by state and federal law
- To public agencies for health oversight activities, such as audits; inspections; civil, criminal, or administrative proceedings; and other activities necessary for the oversight of the health care system
- To law enforcement officials
- For judicial and administrative proceedings, if the request for information is made through a court order
- For research

De-identification indicators (US)

- De-identified information does not qualify as PHI, and therefore is not protected under the Privacy Rule—it can be disclosed to researchers at any time.
- The HIPAA offers two methods to de-identify personal health information.
  - Under the statistical method, a statistician or person with appropriate training verifies that enough identifiers have been removed that the risk of identification of the individual is “very small”- Expert Determination.
  - Under the “safe harbor” method, data are considered de-identified if the covered entity removes 18 specified personal identifiers from the data

Proposed Policy

- Disclosure without obtaining consent, along with personally identifiable information, would be made permissible under certain limited circumstances including mandatory disclosure and for research purposes.
- The mandates where such disclosures would be specified (partially through subsequent guidelines).
- For anonymization and de-identification standards would be framed (through subsequent guidelines).
- The competent authority to make these determinations should be trained in this regard.
- The US position where “waiver of authorization” i.e. wherein requirement of consent is waived, after the decision of the IRB/Privacy Board is proposed to be adopted.

Cyber Security & Cybercrime

NHS cyber-attack: GPs and Hospitals hit by Ransomware -13th May 2017

- NHS services across England and Scotland have been hit by a large-scale cyber-attack that has disrupted hospital and GP appointments.
- The prime minister said the incident was part of an untargeted wider attack affecting organisations globally.
- Some hospitals and GPs have been unable to access patient data, after their computers were locked by a ransomware program demanding a payment worth £230.
- But there is no evidence patient data has been compromised, NHS Digital said.
- The BBC understands about 40 NHS organisations and some GP practices have been hit. The NHS in Wales and Northern Ireland has not been affected.
- There is no indication of who is behind the attack yet, but the hackers demanded their payment in the virtual currency Bitcoin, which is harder to trace.
- Prime Minister Theresa May said: "This is not targeted at the NHS, it's an international attack and a number of countries and organisations have been affected.“

Source: http://www.bbc.com/news/health-39899646

Cyber Security Policy (Sri Lanka)

- **High Level IS Policy**
- **Part of e-Gov Policy**
  - Based on ISO 27001
  - 17 domains covering most of the areas in Information Security
  - Is the Health Sector Organizations taking this seriously??

Cyber – Hygiene “Herd- Immunity”

NotPetya ransomware attack

Corporate social responsibility should include cyber security

Scott Shackelford

This terminal at the main post office of Ukrainian postal service Ukrposhta was one of the casualties of the NotPetya ransomware attack that affected many institutions in the country on Tuesday. Such incidents highlight the vital need for companies to take cyber security seriously, says the writer. PHOTO: EUROPEAN PRESSPHOTO AGENCY

As the NotPetya ransomware attack spreads around the world, it's making clear how important it is for everyone – and particularly corporations – to take cyber security seriously.

The companies affected by this malware include power utilities, banks and technology firms. Their customers are now left without power and other crucial services, in part because the companies did not take action and make the investments necessary to better protect themselves from these cyber attacks.

Cyber security is becoming another facet of the growing movement demanding corporate social responsibility. This broad effort has already made progress towards getting workers paid a living wage, encouraging companies to operate zero-waste production plants, and practise cradle-to-cradle manufacturing.

The overall idea is that companies should make corporate decisions that reflect obligations not just to owners and shareholders, customers and employees, but to society at large and the natural environment.

As a scholar of cyber-security law and policy and chair of Indiana University's new integrated programme on cyber-security risk management, I say it's time to add cyberspace to that list.

ONLINE SECURITY AFFECTS EVERYONE

The recent WannaCry ransomware attack affected more than 200,000 computers in 150 nations.

The results of the attack made clear that computers whose software is not kept up to date can hurt not only the computers' *owners, but ultimately all Internet users. The companies hit by the* Department of Homeland Security, the chief federal agency dealing with cyber security, has highlighted businesses' "shared responsibility" to protect themselves against cyber attacks.

Consumers can't protect their utility services, banking systems or even their personal data on their own, and must depend on companies to handle that security.

Cyber security is an effort that not

VACCINATING CYBERSPACE

If more companies get serious about cyber security, the Internet ecosystem will be safer for everyone.

The concept is much like vaccinating people against disease: If enough people are protected, the others benefit too, through what is called "herd immunity".

In terms of deterring hackers, the number of vulnerable targets will an important step in developing a global culture of cyber security.

Customers can get involved in this effort, demanding better cyber security from companies they do business with.

These can include online retailers, whether small specialised sellers or giants like Amazon.

But local brick-and-mortar stores with customer loyalty programmes that have built their brands on trust mobile apps for privacy and cyber security.

Advocacy groups like the Internet Society and many others should ask companies to discuss cyber-security efforts in their reports to shareholders. And they should urge government agencies to develop voluntary programmes like the US Environmental Protection Agency's Energy Star huge role in shaping the future of our shared experience online.

Cyber security and data privacy are key elements of this, and it's time consumers demand corporations treat them as the 21st-century social responsibilities they are.

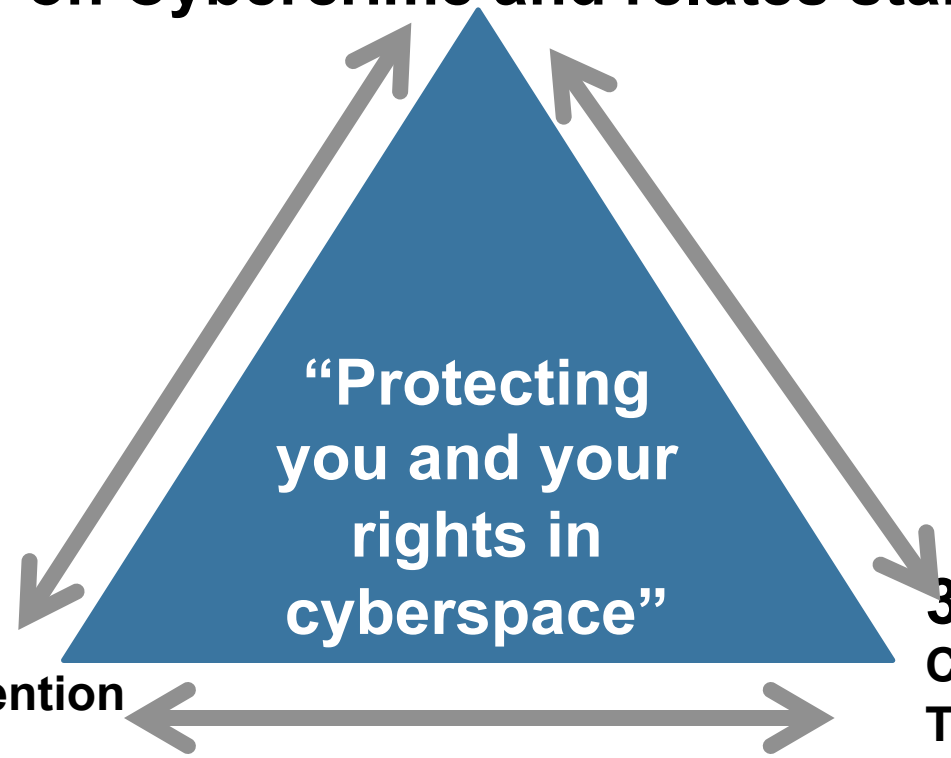
• The writer is an associate professor of business law and ethics, director,

Cybercrime : Global Challenge

- Multi jurisdictional in Nature
  - Actions of criminals can reach computers/ devices and victims in many other countries
  - Evidence in multiple countries (“Evidence in the Cloud”)
  - Where was the offence committed and which Country has jurisdiction
  - Need for global Legislative standard, tool for Judicial Collaboration

The Budapest Cybercrime Convention

1 Common standards: Budapest Convention on Cybercrime and relates standards



2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Legal & Institutional Frameworks – Sri Lanka

- Computer Crimes Act No. 24 of 2007 etc
- Sri Lanka's Entry into the Budapest Cybercrime Convention
  - 1st September 2015

- Sri Lanka CERT – www.slcert.gov.lk
  - National Centre for Cyber Security
  - Launched Sector specific CSIRTS (eg:- Bank CSIRT with Central Bank & Banking Sector) - **FinCERT**
  - A Public private partnerships model to protect critical information infrastructure
  - National Cyber Security Strategy (2019-23)

- "Digital Crimes" & "Digital Forensic" at Cyber Crime Unit of CID – Sri Lanka Police

Summary

- The proposed policy is a framework in relation to protection and use of data.
- Subsequent guidelines would be needed to strengthen the framework.
- Enforcement and penalties for non-compliance are still grey areas which need to be addressed.
- Establishes a framework to better implement Section 5 of RTI Act

"The duty to share information can be as important as the duty to protect patient confidentiality"

UK Caldicott Principles