Version 2

Discussion Paper on Healthcare Data Protection Policy for Sri Lanka[1]

Ashwini Natesan, Sriganesh Lokanathan, Rohan Samarajiva, Sunali Jayasuriya, Mohamed Haniffa Abusayeed, Jayantha Fernando

LIRNEasia & ICTA

20 May 2019

The research and preparation of this discussion paper has been funded by LIRNEasia, the International Development Research Centre (IDRC) of Canada, and ICTA.

Table of Contents

(I) Background 3
(II) Rationale for healthcare data protection policy 3
(III) Current context in Sri Lanka 4
Position in Sri Lanka in relation to privacy and data protection 5
IV) Healthcare data protection in other jurisdictions 6
(V) Scope of healthcare data 7
Rationale for defining healthcare data 7
Proposed scope for entities that will be governed by the new policy in Sri Lanka 11
Proposed definition of healthcare data for Sri Lanka (Adopted from the UK Data Protection Act and Australia's Privacy Act) 12
Items for discussion 13
(VI) Healthcare Data Protection 15
Existing healthcare data protection in Sri Lanka 15
Personal data 16
Identified or identifiable individual 17
Confidentiality of healthcare data 18
Healthcare data protection obligations in studied jurisdictions 18
Europe/GDPR 19
India 20
Australia 20
UK 21
Singapore 21
Proposed framework of applicable healthcare data protection obligations for Sri Lanka 22
Processing of personal data 24
Data owner/principal, data controller, and data processor 25
Prior consent to disclose information 25
Additional considerations for healthcare data protection for Sri Lanka 27
Items for further discussion 27
Information not personally identifiable 27
(VII) Disclosure of healthcare data for research 27
Pseudonymization and anonymization 27
Proposed framework for processing data for research purposes in Sri Lanka 31
(VIII) Mandatory Disclosure 33
Existing Sri Lankan context 33
Comparative Positions 33
Mandatory disclosure for research purposes 35
Items for further discussion 35
(IX) Additional areas for discussion 36
Measures required to ensure information security 36
Enforcement of policies and penalties for non- compliance 36
Subsequent guidelines (the committees formed under the National Policy on Health Information) 36
Guidelines for "primary business" and a committee for issues arising thereon 36

(I) Background

1. There is increasing need for management of healthcare data, its protection, and use. A framework for data protection and use is essential particularly since momentum for use of healthcare data has been increasing across jurisdictions. Some prior work has been done in relation to this in Sri Lanka, with a policy for health information being adopted in 2017. In line with the government's intention to lay down policies for protection of healthcare data, this discussion paper highlights, amongst others, issues in relation to healthcare data protection.

2. The demand for the use of patient healthcare data for secondary purposes, i.e. uses not directly related to a specific treatment and care of a specific patient, is growing. The potential for big data analytics and artificial intelligence (AI) to reveal underlying patterns and associations has tremendous implications for many healthcare related fields, such as epidemiology, risk management, and health research, and facilitate the significant discoveries that could advance medical knowledge, medicine, and medical treatment, amongst others.

3. Sri Lanka has been increasingly moving towards adapting Electronic Medical Records (EMR) both in the government and private sector. More than 50 government hospitals currently use EMR for outpatient records and a large number of private hospitals also use EMR for several purposes. The rising adoption of EMR increases the need for a functioning data protection policy.

4. This discussion paper seeks to articulate a broad framework that would both help facilitate healthcare data protection as well as facilitate the use of healthcare data to improve individual as well as well as public health.

(II) Rationale for healthcare data protection policy

5. The rationale and necessity for a healthcare data protection policy is predicated on the increased role of, and collection of, personal data in the world. Existing principles and mechanisms for the protection of personal data and their use are likely to undergo a sea change. As outlined in a 2012 OECD report, several changes in the last 30 years necessitate the need for a healthcare data protection policy.[2] And specifically in relation to Sri Lanka the rationale for the need for a healthcare data protection policy include:

   a) The increased volume of personal healthcare data being collected, used and stored;

[2] The OECD Report On The Work Of The Working Party On Information Security And Privacy Group Of Privacy Experts In Connection With The Review Of The 1980 OECD Privacy Guidelines is available from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2012)15/FINAL&docLanguage=En

b) The increasing accessibility to analytics that can provide insights into individual and group trends, movements, interests, and activities;

c) The value of the societal and economic benefits enabled by new technologies and responsible data uses;

d) The extent of threats to privacy;

e) The number and variety of actors capable of either putting privacy at risk or protecting it;

f) The frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate;

g) The global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows;[3]

h) The secondary uses of healthcare data in medical research and advanced medical care;

i) The lack of a framework for healthcare data protection;

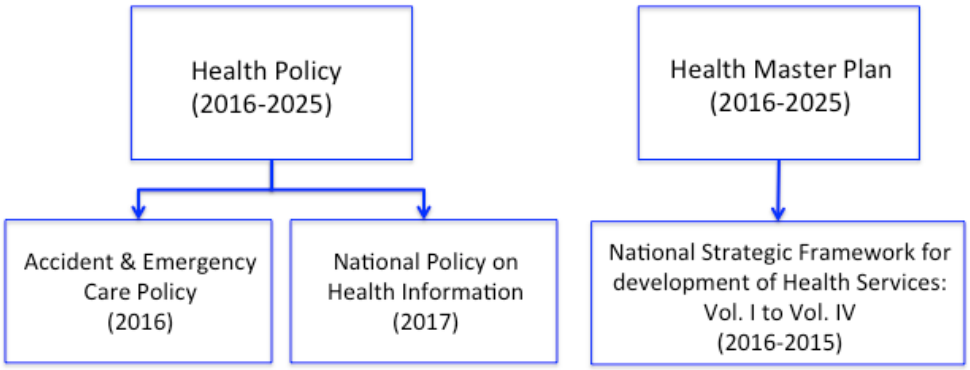
j) The need for a scheme that can ensure information are not only protected but also shared for better care and research; and

k) The need for policy coherence.

(III) Current context in Sri Lanka

6. A coherent policy framework for the protection of healthcare data does not currently exist in Sri Lanka. Neither does Sri Lanka have a comprehensive data protection framework (though work has begun on developing comprehensive data protection legislation). A patchwork of policies and guidelines do cover some aspects of data protection and data use in relation to healthcare data/ information. In studying the relevant laws, policies, regulations, and guidelines, the following diagrams attempt to depict some relevant linkages.

[3] Items (a) to (g) quoted verbatim from the OECD Report On The Work Of The Working Party On Information Security And Privacy Group Of Privacy Experts In Connection With The Review Of The 1980 OECD Privacy Guidelines available at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2012)15/FINAL&docLanguage=En



7. In addition the following are also of relevance to the domain of health information:

- 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)

8. The National Policy on Health Information 2017 ["Health Information Policy") lays down directives in relation to:

- Health information related resources
- Indicators and data elements
- Data and Information management
- Data / information security, client privacy, confidentiality and ethics
- e-health and innovations

Position in Sri Lanka in relation to privacy and data protection

9. There is currently no constitutional right to privacy. Article 14A the Constitution deals with the right of access to information. In the said provision, privacy is included as an exemption, wherein information requested can be refused on the grounds that it violated privacy. It is to be noted that where as the right to access of information is a fundamental right, privacy is only included as an exemption. Furthermore, if the public interest of the people outweighs the right to privacy, that right outweighs the latter. Therefore, the right to privacy is connected to the right to information and fails to stand on its own. As such, there is no express provision where the right to privacy is a separate and compounded fundamental right of the citizens in Sri Lanka. Also in order for this right to be exercised against private organisations, a statute would be needed, where it would have to be encapsulated separately.

10. Under the Right to Information Act No. 12 of 2016, which has its root in the Constitution of Sri Lanka, privacy is an exemption under section 5.[4] Here again privacy is not an enforceable right but is stated as one of the grounds to refuse disclosure of information. The Right to Information Commission has in several instances prohibited disclosure of information if the requested information infringes the privacy of an individual.

11. There are certain other provisions in relation to data protection measures in other legislations. It is pertinent to note that the provisions mentioned below are sector specific with limited application:

- 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).

12. The E-Government Policy does not state in detail about the data protection requirements but has a generic inclusion which states as follows:

- Processing/ Retention/ release of personal data and information should be in accordance with applicable laws and regulations.
- Email addresses of citizens collected through government websites should not be divulged.

13. In relation to the 2017 National Policy on Health Information,

- The Director General of Health Services, Deputy Director General (ET&R), Deputy Director General (Planning) have been given the responsibility to establish guidelines for the collection of individually identifiable information.
- The Director of Health Information and Deputy Director General (Planning) have been given the responsibility to design and use a Personal Health Number (PHN) for client identification and preserving confidentiality and privacy. It is pertinent to note that the eHealth Guidelines and Standards, 2016 also provides for the issuance of PHN number.
- The Director General of Health Services, Director of Health Information, and Deputy Director General (Planning) have been given the responsibility of educating staff on concepts of anonymity and pseudonymity.

IV) Healthcare data protection in other jurisdictions

[4] Section 5 (1) (a) of the Right to Information Act reads: "the information relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the larger public interest justifies the disclosure of such information or the person concerned has consented in writing to such disclosure."

14. The table below outlines the various jurisdictions that have been studied and their approach towards healthcare data protection.

Jurisdiction	Summary of Approach	Legislation(s) studied
EU	• Comprehensive data protection framework (that includes healthcare data). • Rights based approach- individual at the center of law. • Applies to processing of personal data and covers both private sector as well as government.	• General Data Protection Regulation ["**GDPR**"], 2016/679
• **USA**	• Sectoral data protection framework; for medical data, the federal legislation applies.	• Health Insurance Portability and Accountability Act of 1996 ["**HIPAA**"]
Australia	• General legislation on privacy. Separate regimes for public and private sectors.	• The Privacy Act 1988
UK	• General legislation on data protection.	• Data Protection Act 2018
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 has been published, but has not yet been adopted.	• Draft Data Protection Bill 2018 • Draft Digital Information security healthcare act ["**DISHA**"]
Singapore	• General data protection legislation; advisory guidelines for health sector	• Personal Data Protection Act 2012 ["**PDPA**"]

(V) Scope of healthcare data

15. The discussion paper aims to delineate the scope to reduce regulatory burden and ensure that data protection obligations are introduced in a phased manner to different players who will be governed by the policy. Furthermore, the National Health Information Policy did not include a definition / scope as to the application of the same. Hence, this section bears relevance not only in terms of the proposed healthcare data protection policy but also to ensure implementation of the 2017 National Policy on Health Information.

Rationale for defining healthcare data

16. There are several important reasons to define healthcare data:

a) To regulate institutions who would be governed by the policy
The 2017 Health Information Policy has dealt with "health information." Whereas the policy states that the requirements enshrined thereunder would be applicable to both private and public entities, yet no definition has been included as to what constitutes health information. In contrast, international jurisdictions analysed in this discussion paper have defined what constitutes health information albeit in different ways.

b) To regulate institutions providing "healthcare" and/or "healthcare related services"
The regulation of "health information" can be on the basis of a) type of information (whether the information constitutes "health information/ data" or b) the entity in whose possession such information is held. It is noted that several kinds of information would be generated pertaining to health and instead of ambiguously and inclusively defining such "health information," it could be defined on the basis of the entities generating / possessing the relevant healthcare data. For example the GDPR broadly defines the subject matter as "health concerning data."

c) Avoid overarching application to allied industries
Health related activity-monitoring devices (for example Fitbit) collect health-related data, but it is not feasible to bring such international equipment manufacturers under the purview of a Sri Lanka specific legislation. This discussion paper aims at laying down a framework for regulating organisations, which deal with healthcare data as a "primary" business. The test for what constitutes primary business has not, however, been laid out within this discussion paper.

17. The table below summarizes how healthcare data has been defined across jurisdictions

Jurisdiction	Provision	Comments
GDPR	"**Data concerning health**" is defined by the GDPR as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."	The GDPR treats health data (widely defined) as sensitive personal data. Recital 35 of the GDPR is of relevance in this regard: "*Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU (relates to patients' rights in cross-border healthcare) of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data*

Jurisdiction	Provision	Comments
		and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test." Note the GDPR now specifically lists genetic data and biometric data as sensitive personal data and permits Member States to introduce further conditions around the processing of biometric, genetic, or health data.
UK Data Protection Act 2018	<u>Section 205</u> <u>Meaning of health record: "</u> *a record which:* *a) Consists of data concerning health, and* *b) Has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;"* <u>Section 204</u> Meaning of health professional: " *a) A registered medical practitioner;* *b) A registered nurse or midwife;* *c) A registered dentist within the meaning of the Dentists Act 1984 (see section 53 of that Act);* *d) a registered dispensing optician or a registered optometrist within the meaning of the Opticians Act 1989 (see section 36 of that Act);* *e) a registered osteopath with the meaning of the Osteopaths Act 1993 (see section 41 of that Act);* *f) a registered chiropractor within the meaning of the Chiropractors Act 1994 (see section 43 of that Act);* g) *a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 (S.I. 2002/254) for the time being extends, other than the social work profession in England*"	The first limb of the definition is rather wide to include all records that concern health. Made more restrictive in the application in the second part. Thus, (b) would exclude Fitbit data.

Jurisdiction	Provision	Comments
HIPAA	"health information" means any information, including genetic information, whether oral or recorded in any form or medium, that is: *a) Created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; and* *b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.* *A health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.* *Health plan means an individual or group plan that provides, or pays the cost of, medical care. Health plan includes the following, singly or in combination:* *a) A group health plan, as defined in this section.* *b) A health insurance issuer, as defined in this section.* *c) An HMO, as defined in this section.* *d) Part A or Part B of the Medicare program under title XVIII of the Act.* *e) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.* *f) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.* There are a host of other categories.	Wide definition included but the HIPAA is made applicable to "covered entities."

Jurisdiction	Provision	Comments
Privacy Act 1988 (Australia)	Health information means: a) Information or an opinion, that is also personal information, about: (i) The health or a disability (at any time) of an individual, or (ii) An individual's expressed wishes about the future provision of health b) Other personal information collected to provide, or in providing, a health service; or c) Other personal information collected in connection with the donation, their body parts, organs or body substances, or d) Genetic information "Health service" an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it: a) to assess, record, maintain or improve the individual's health; or b) to diagnose the individual's illness or disability; or c) -to treat the individual's illness or disability or suspected illness or disability; or d) -the dispensing on prescription of a drug or medicinal preparation by a pharmacist	The Privacy Act applies to the private sector. State and territory public sector providers such as public hospitals are regulated by State or Territory privacy law. The applicable legislation depends on who holds the records. Examples of health information include: • information about an individual's physical or mental health • notes of an individual's symptoms or diagnosis and the treatment given • specialist reports and test results • appointment and billing details • prescriptions and other pharmaceutical purchases • dental records • records held by a fitness club about an individual • information about an individual's suitability for a job, if it reveals information about the individual's health • an individual's healthcare identifier when it is collected to provide a health service • any other personal information (such as information about an individual's date of birth, gender, race, sexuality, religion), collected for the purpose of providing a health service. Some examples of health service providers include: • General practitioners and medical specialists • Private hospitals and day procedure centers • Pharmacists • Other health and allied health professionals in private practice including psychologists, physiotherapists, dentists, podiatrists, occupational and speech therapists and optometrists • Private aged care facilities • Pathology and radiology services

Proposed scope for entities that will be governed by the new policy in Sri Lanka

18. Since Sri Lanka does not yet have general data protection legislation (though it is presently being drafted), the scope could 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 those come into possession of such health information in the course of their primary business (e.g., insurance companies, as included under the US HIPAA).
- 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.

Proposed definition of healthcare data for Sri Lanka (Adopted from the UK Data Protection Act and Australia's Privacy Act)

19. Two possible definitions are suggested:

- "Healthcare data" constitutes all data or information that are generated, captured, transmitted, stored, processed, analysed, and disseminated on electronic format, pertaining to health of a natural person or healthcare service in Sri Lanka and held by a health professional;

OR

- Any health related information generated, captured, transmitted, stored, processed, analysed and disseminated by individual or an entity whose primary business is to provide healthcare

20. A "health professional" can include one or more of the following:

a) A registered medical practitioner within the meaning of Section 29 of the Medical Ordinance, No: 26 of 1927 as amended;[5]

b) A registered nurse within the meaning of Section 63 of the Medical Ordinance, No. 26 of 1927 as amended;

c) A registered dentist within the meaning of the Section 43 of Medical Ordinance, No. 26 of 1927 as amended;

d) A registered Midwife within the meaning of Section 51 of Medical Ordinance, No. 26 0f 1927 as amended;

e) A registered pharmacist within the meaning of the Section 56(1) of the Medical Ordinance, No. 26 of 1927 as amended;

f) Providing alternative medicine therapies other health and allied health professionals in private practice including psychologists, physiotherapists, dentists, podiatrists, occupational and speech therapists and optometrists;

g) Private aged care facilities;

h) Pathology and radiology services;

[5] A "registered medical practitioner" includes a person who is provisionally registered under section 31 the Medical Ordinance, No. 26 of 1927 as amended.

i) Complementary medicine practitioners, including herbalists, naturopaths, chiropractors, massage therapists, nutritionists, and traditional medicine practitioners;

j) Health services provided in the non-government sector, such as phone counselling services or drug and alcohol services;

k) Child care centres;

l) Gyms and weight loss clinics;

m) Blood and tissue banks;

n) Assisted fertility and IVF clinics; and

o) Health services provided via the Internet (e.g. counselling, advice, medicines), tele-health and health mail order companies.

21. A healthcare service includes:

a) The Department of Health which consisted of Division of Medical Services, Division of Public Health Services and Division of Laboratory Services in relation to the exercise of functions under section 5 of the Health Services Act, No. 12 of 1952 as amended;

b) The Health Council established under Section 4 of the Health Services Act, No. 12 of 1952 as amended;

Items for discussion

22. Several aspects require further discussion at the consultation stage:

a) Should the territorial application of the policy be extended?

- The question of extra territorial application of a policy is intrinsically tied to enforcement. While enforcing the proposed policy obligations within Sri Lanka is in itself a challenge unless such power is derived from the constitution or a statue, extra territorial enforcement by a small country like Sri Lanka is much more difficult.
- Cross border transfers of data by entities in Sri Lanka is also relevant to this question, but for the purposes of this discussion document, that issue is dealt with later in the section on data protection obligations.
- For data controlled and processed (these terms have been defined in the next section) outside Sri Lanka, this discussion paper has not suggested any mechanism of regulation. The regulation of such entities may potentially be considered in a phased manner.

b) Should the definition of health professional be extended to include additional entities?

- The proposed “health professional” definition is inclusive and not exhaustive. It is understood that several other organisations such as educational institutions also possess healthcare data. As such it should be considered whether these additional entities should also be included in an expanded definition.

c) How should health information of employees held by companies be treated?
    - It is not uncommon for businesses (other than those engaged in healthcare) to collect health information of employees. How should such health information collected by secondary organizations be dealt with?

d) How should paper-based records be dealt with?
    - Till recently, much of the existing healthcare data in Sri Lanka was in paper based form. Data protection of such paper based health records is another area that needs to be addressed either through this policy or subsequently.

(VI) Healthcare Data Protection

Existing healthcare data protection in Sri Lanka

23. Some aspects of healthcare data protection are currently covered under the 2017 National Policy on Health Information, Section 4 on "Data/Information Security, Client Privacy, Confidentiality and Ethics" which states the following:

    a) "*Ethical and fair information practices shall be incorporated into information management ensuring client privacy and confidentiality*" (Section 4.1)

    b) "*Data and information security shall be ensured for client data protection*" (Section 4.2)

24. While the 2017 National Policy on Health Information is not specific on how the above provisions are to be carried out, the 2016 National eHealth Guidelines and Standards V1 under the section on "Privacy and confidentiality" gives more detail:

    a) "*Ensure confidentiality of personally identifiable data and information at all stages of the Health Information Systems (HIS) cycle*" (Section 5.2.1)

    b) "*Personally identifiable data and information shall be used only for the purpose for which the data was collected. If such data is to be used for any other purpose, a proper de-identification procedure shall be followed*" (Section 5.2.2)

    c) "*Unless disclosure is enforced by law, personally identifiable information should not be disclosed without written informed consent of the individual concerned for any other purpose than the purpose for which it was collected for*" (Section 5.2.3)

    d) "*Health care workers access to healthcare related information should be strictly on a need-to-know basis and such access should be revoked immediately when the job role is changed or is terminated*" (Section 5.2.4)

    e) "*Role based access control profiles should be clearly defined and documented*" (Section 5.2.5)

    f) "*It is the duty of Healthcare Institutions to ensure that information of an individual is accessible only to employee/s who have signed an information confidentiality agreement (Non-Disclosure Agreement)"* (Section 5.2.6)

    g) "*Healthcare institutions shall ensure that employees who leave the organization are bound to maintain confidentiality of information that they have come to know during the period of employment with the institution*" (Section 5.2.7)

    h) "*Healthcare institutions shall ensure that third party personnel involved with health information systems including maintenance should sign non-disclosure agreements*" (Section 5.2.8)

    i) "*An individual has the right to appeal for amendments to personal information held in an information system in the event of any discrepancy*" (Section 5.2.9)

Personal data

25. Data protection principles are designed to protect the personal data/information of individuals by restricting how such information can be "processed" including but not limited to collection, use, and disclosure.

26. Health data is classified as "personal data" in foreign jurisdictions (UK, US, Australia, India, and Singapore were specifically studied). In the studied jurisdictions health / healthcare data are subject to additional compliance requirements due to sensitive nature, and which are outlined in the table below:

Legislation	Provision	Comments
GDPR	Article 4 of the GDPR states as follows: • *'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*	Health data is considered sensitive personal data
Australia Privacy Act	Personal data includes • *"…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable"*	
India – Draft Data Protection Legislation	• *Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information*	Health data is considered sensitive.
HIPAA	HIPAA uses the term 'Protected health information' that is defined as individually identifiable health information transmitted or	The definition exempts a small number of categories of individually identifiable health information, such as individually identifiable health information found in employment records held by a covered entity in its role as an employer

Legislation	Provision	Comments
	maintained by a covered entity[6] or its business associates in any form or medium.	
Singapore – PDPA	*"Personal data" means data, whether true or not, about an individual who can be identified —* *a) from that data; or* *b) from that data and other information to which the organisation has or is likely to have access;*	Advisory guidelines issued for personal data and specifically for healthcare organisations.
UK - Data Protection Act 2018	*"Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c))*[7] *"Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—* *a) an identifier such as a name, an identification number, location data or an online identifier, or* *b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.*	

Identified or identifiable individual

27. From all the definitions outlined earlier it is clear that personal data are those data / information with which a person may be identified. Distinction has to be made between healthcare data where personal information is identifiable and where they are not (i.e. anonymized / de-identified). The principles of confidentiality, consent, and other data protection obligations are applicable to healthcare data, which are "personally identifiable." The exceptions to this rule and rules in relation to anonymization and de-identification will be discussed in the next section.

28. All information about an individual is not personal data. Protection of identity is central to informational privacy. So the information must be such that the individual is either identified or identifiable from such information. In statutes or instruments which use both these terms (i.e. "identified" or "identifiable") such as the GDPR, it refers to states in which the data could be in a form where individuals stand identified or in other cases, it is possible that they could be identified. Whether an individual is identifiable or not is a

[6] Detailed definitions and explanations of these covered entities and their varying types can be found in the "Covered Entity Charts" available through the OCR website, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.

[7] References to personal data, and the processing of personal data, are to personal data and processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.

question of context and circumstance. For instance, a car registration number, by itself, does not reveal the identity of a person. However, it is possible that with other information, an individual can be identified from this information.[8]

29. In the (Australian) Privacy Act, the definition of personal information makes the standard of "reasonably identifiable" explicit. "Personal information", under the Privacy Act means information or an opinion about an identified individual or an individual who is reasonably identifiable. Another example is the Data Protection legislation in Canada, goes a step further and drops the term 'identified' from the scope of the definition entirely and refers only to information about an identifiable individual.

Confidentiality of healthcare data

30. All analyzed jurisdictions mandate confidentiality of healthcare data, which are considered sensitive personal data. Additionally, the International Code of Ethics of the World Medical Association (WMA) makes respecting the right to confidentiality a duty integral to a physicians' responsibility to patients. The WMA Declaration of Helsinki—Ethical Principles for Medical Research Involving Human Subjects (revised 2013) places a duty on physicians "to protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects … even though they have given consent."[9] Recognizing that this personal information, whether collected for research or clinical practice, is increasingly held in databases, in 2002 the WMA adopted the Declaration on Ethical Considerations Regarding Health Databases: "Confidentiality is at the heart of medical practice and is essential for maintaining trust and integrity in the patient-physician relationship. Knowing that their privacy will be respected gives patients the freedom to share sensitive personal information with their physician." This discussion paper aims at laying down instances where information can be disclosed and the obligations vested on healthcare organisations.

Healthcare data protection obligations in studied jurisdictions

31. The different jurisdictions studied have varied approaches towards healthcare data protection obligations, which are summarized in the table below, and then addressed in more detail subsequently on a per jurisdiction basis.

Legislation/ Jurisdiction	Provision	Comments
GDPR	Health data (considered as sensitive data) cannot be processed unless explicit consent has been obtained, or presence of other	The GDPR encompasses wide obligations. The proposed model for Sri Lanka does not replicate such wide obligations

[8] 2017 White Paper of the Committee of Experts on a Data Protection Framework for India

[9] World Medical Association. Declaration of Helsinki—Ethical Principles for Medical Research Involving Human Subjects; available at http://www.wma.net/en/30publications/10policies/b3

Legislation/ Jurisdiction	Provision	Comments
	overriding considerations like public interest, scientific research etc.	
India	The Data Protection Bill 2018 encompasses in great detail the data protection principles. The DISHA (Draft legislation) deals with data ownership, security and standardization.	Certain guidance has been obtained from the draft legislation.
Australia	Health data is classified as "sensitive." The Australia Privacy Principles lay down data protection obligations.	The Australian data privacy principles especially guidelines in relation to anonymization are of relevance.
UK	The Data Protection legislation includes obligations. The Caldicott Privacy Principles are of relevance.	The UK legislation follows GDPR. The Caldicott principles are discussed in detail
US	The Privacy Rule of the HIPAA provides for data protection of protected health information.	The Privacy Rule of HIPAA is detailed and comprehensive. Some guidance has been taken from this for the proposed Sri Lankan model.
Singapore	General data protection legislation; issued advisory guidelines for the health sector	The Singapore model has been adopted to a large extent in the context of Sri Lanka

Europe/GDPR

32. As per Article 6 of GDPR, one of the legal bases for processing of personal data is if "*the data subject has given consent*." Additionally, the following are the *legal bases* for processing personal data:

- It is necessary for the performance of a contract to which the data subject is party;
- It is necessary for compliance with a legal obligation;
- It is necessary to protect the vital interest of the data subject or another natural person;
- It is necessary for the performance of a task carried out in the public interest;
- It is necessary for the purposes of the legitimate interests pursued by the controller or third party.

33. "Health data" is referred under "special categories of data," wherein processing would not only need to be under one of the legal bases listed above (Para 32) but also comply with one of the conditions under Article 9 of the GDPR. The first condition under the said article is that of "explicit consent". It should be noted that "explicit consent" has not been defined under the GDPR. Some of the other conditions, of relevance to processing of health data are:

- To protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- For reasons of substantial public interest,;
- For the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the Member State or pursuant to contract with a health professional and subject to the conditions and safeguards;
- For reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR.

India

34. India's 2018 proposed Personal Data Protection Bill classifies health data as "sensitive personal data" and imposes the following data protection obligations:

- Fair and reasonable processing
- Purpose limitation
- Collection limitation
- Lawful processing
- Notice
- Data quality
- Data storage limitation
- Accountability

Australia

35. Australia's Privacy Principles cover the following areas:[10]

- Open and transparent management of personal information
- Anonymity and pseudonymity
- Collection of solicited personal information
- Dealing with unsolicited personal information

[10] For the full details of each area see https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

- Notification of the collection of personal information
- Use or disclosure of personal information
- Direct marketing
- Cross-border disclosure of personal information
- Quality of personal information
- Security of personal information
- Access to personal information
- Correction of personal information

UK

36. UK's principles are more commonly known as the Caldicott Principles based on the 1997 Caldicott Report that reviewed how patient information were handled across UK's National Health Service. These principles are:

    - Justify the purpose
    - Do not use personal confidential data unless it is absolutely necessary
    - Use the minimum necessary personal confidential data
    - Access to personal confidential data should be on a strict need-to-know basis
    - Everyone with access to personal confidential data should be aware of their responsibilities
    - Comply with the law
    - The duty to share information can be as important as the duty to protect patient confidentiality

Singapore

37. Singapore imposes 9 obligations in relation to data protections. They are outlined in greater detail below:

    a) **Consent Obligation**
    An organisation shall only collect, use or disclose personal data for purposes for which an individual has given his or her consent

    b) **Purpose Limitation Obligation**
    An organisation may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

    c) **Notification Obligation**
    An organisation is required to notify individuals of the purposes for which it intends to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.

    d) **Access and Correction Obligation**

Upon request, the personal data of an individual and information about the ways in which his or her personal data has been or may have been used or disclosed within a year before the request should be provided. However, organisations are prohibited from providing access if the provision of the personal data or other information could reasonably be expected inter alia to cause harm to the safety of the individual or another individual, reveal personal data of another individual, be contrary to national interest etc.

Organisations are also required to correct any error or omission in an individual's personal data upon his or her request.

e) **Accuracy Obligation**
An organisation must take reasonable efforts to ensure that personal data collected by or on behalf of the organisation are accurate and complete, especially if such personal data is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organisation.

f) **Protection Obligation**
An organisation is required to make reasonable security arrangements to protect the personal data that are under its possession or control to prevent unauthorised access, collection, use, disclosure or similar risks.

g) **Retention Limitation Obligation**
An organisation shall cease to retain personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose.

h) **Transfer Limitation Obligation**
Transfer of personal data outside of Singapore is permissible only according to the requirements prescribed under the regulations, to ensure that the standard of protection provided to the personal data so transferred will be comparable to the protection under the PDPA, unless exempted by the Personal Data Protection Commission.

i) **Openness Obligation**
The organisation is required to make information about its data protection policies, practices and complaints process available on request. Also designate one or more individuals as a Data Protection Officer to ensure that the organisation complies with the PDPA

Proposed framework of applicable healthcare data protection obligations for Sri Lanka

38. All analysed jurisdictions have wide healthcare data protection obligations. Obligations such as prior consent, notification, and data integrity have been included in the respective data protection legislation. Since Sri Lanka does not have any specific data protection obligations in place (a comprehensive data protection law is currently being drafted), it is proposed that certain basic and important requirements be enshrined. These are by no means exhaustive and may be considered as a first step in developing a more comprehensive data protection policy.

39. Some of the Singapore PDPA principles are proposed for adoption by virtue of them being simple and often-considered "baseline" protection. Furthermore the UN Principles on Personal Data Protection and Privacy, setting out the basic framework for the processing of personal data by, or on behalf of, the United Nations System Organizations, embody several of the principles included below.[11]

40. The proposed data protection obligations are enumerated below:

a) Confidentiality
healthcare data shall be subject to strict confidentiality. The relevant personally identifiable healthcare data shall not be disclosed unless the various obligations given below are satisfied

b) Consent Obligation
The data controller can only process data only after obtaining consent. *Informed consent*, elaborated below

c) Purpose Limitation Obligation
The data controller can only use healthcare data for the purposes disclosed and for which prior consent has been obtained. Consent obtained can be used for several purposes provided the same has been mentioned in clear and unambiguous language.

d) Notification Obligation
If data is being processed for ancillary or other related purposes the data owner has to be notified.

e) Access and Correction Obligation
Upon request, the personal data of an individual and information about the ways in which his or her personal data has been or may have been processed within a year before the request should be provided. However, data controller is prohibited from providing access if the provision of the personal data or other information could reasonably be expected inter alia to cause harm to the safety of the individual or another individual, reveal personal data of another individual, be contrary to national interest etc.

Data controller is also required to correct any error or omission in an individual's personal data upon his or her request.

f) Accuracy Obligation
The data controller must take reasonable efforts to ensure that personal data collected by or on behalf of the organisation are accurate and complete, especially if such personal data is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organization.

g) Integrity & Protection Obligation

[11] The complete list of UN principles can be found at https://www.unsceb.org/principles-personal-data-protection-and-privacy

The data controller is required to security arrangements to protect the personal data that are under its possession or control to prevent unauthorised access, collection, use, disclosure or similar risks.

h) Retention Limitation Obligation
The data controller shall cease to retain personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose.

i) Openness Obligation
Data controllers are required to develop a policy in relation to processing of healthcare data. The data controllers are also required to make information about its data protection policies, practices and complaints process available on request

Processing of personal data

41. Under the GDPR and the Draft Data Protection Bill 2018, distinction is made between data controllers and processors. In simple terms data controllers refers to those entities who require the heath data for example the hospital, the data processor is the third party entity who "processes" the personal data on behalf of the controller.

42. Similarly HIPAA only applies to "covered entities." While the covered entities are core participants in the industry, they rely on tens of thousands of vendors to provide them services, with many of these services involving patient information.[12] To resolve this conundrum, the concept of a 'business associate' was included wherein an entity that provides services to the healthcare industry where the performance of those services involves the use or disclosure of patient information.[13] Although the US Department of Health and Human Services (HHS) has no direct jurisdiction over these 'business associates,' HHS imposes an obligation on the covered entities to implement specific contracts with these vendors that would create contractual privacy and security obligations for these vendors. The failure to execute a contract would mean that the covered entity violated the HIPAA rules. This system has existed since the inception of the HIPAA Privacy Rule in 2003.

43. The definition under the GDPR is as follows: *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"

44. For Sri Lanka, it is proposed that the GDPR definition of processing be adopted since it is comprehensive and wide.

[12] Analyzing the US HIPAA legacy and future changes on the horizon D.P.L. & P. 2013, 10(2), 14-16

[13] Ibid.

Data owner/principal, data controller, and data processor

45. The individual whose data is collected is the data owner. The "data principal" definition in the Draft Data Protection Bill (India) is useful. The definition simply states that the individual whose data is collected is the "data principal."

46. In today's context it is essential to cater to the possibilities of different organisations handling processing of data. Guidance has been taken from the GDPR in this regard to ensure those third party entities are also subject to certain data protection obligations indirectly. The definitions under the GDPR encompass definitions that are unambiguous and succinct. Further the GDPR definition is consistent with those adopted in UK and India.

47. Article 4 of the GDPR defines a *data controller* as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*" It also defines a data processor as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*."

48. In Sri Lanka's context the above definitions may be adopted. In general the data controller will be required to comply with all the obligations (as is the case with GDPR). Certain responsibilities have to be imposed on the data processor as well. For instance the obligation under Article 28(1) of the GDPR states that "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."*

49. The proposed framework for Sri Lanka should include similar guarantees that are imposed on data controllers to ensure that the data protection obligations would be complied with by the data processors.

50. The following definitions are proposed in the Sri Lankan context:

    a) 'Data principal' means the natural person to whom the personal healthcare data relates.

    b) 'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

    c) 'Data processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

Prior consent to disclose information

51. There are various definitions of *consent* amongst the different jurisdictions that were studied. The following are of relevance for the purposes of understanding *consent*

- 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (as defined by GDPR).
- The PDPA (Singapore) holds that for "consent" to be considered valid a) notification of purpose and b) use of information for that purpose *only*, are mandatory.
- Under the Draft Data Protection Act (India) sensitive personal data (such as health data) can be processed only after obtaining 'explicit consent.' In addition to the general requirements of "consent"[14] for compliance of "explicit consent" requirement the same should be informed, clear and specific.

52. All analysed jurisdictions mandate prior consent to "process" personal data.

53. In the Sri Lankan context, it is proposed that 'informed consent' be obtained to process healthcare data. The Draft Mental Health Act of Sri Lanka (2007) by Ministry of Health provides a basis for the definition of 'informed consent' that can also be adopted for this policy.

- As per Section 94 of the Draft Mental Health Act, "'informed consent' *means consent obtained freely, without threats or improper inducements, after appropriate disclosure to the patient of adequate and understandable information in a form and language understood by the patient and as further defined by prescribed regulation"*

54. In the case of persons who cannot give consent, consent can be obtained from the parent, guardian, or next of kin as the case may be. Persons who cannot give consent include:

a) Those of unsound mind
b) Minors
c) Dead persons
d) Those unable to provide consent

55. Healthcare data may be processed without consent if:

a) The processing is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent.
b) The processing is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual.

[14] Section 12 defines consent as valid if given- freely (without any undue influence); informed disclosing all relevant information; specific (having regard to the scope of consent); clear indicated through affirmative action and capable of being withdrawn.

Additional considerations for healthcare data protection for Sri Lanka

56. In formulating a healthcare data protection framework for Sri Lanka, it is proposed that the following be also adopted:

    a) Be applicable to both *private* and *public* heath sectors

    b) *Data minimization* (processing of only data that is required for the purpose)

    c) Utilization of *Informed consent* for personally identifiable healthcare data

    d) Ensure *controller accountability* (making the data controller accountable for any processing of data)

    e) *Technology agnosticism* (adopt a technology neutral stance to take into account changing technologies and standards of compliance)

    f) Framing of subsequent regulations to *ensure compliance.*

Items for further discussion

57. The following questions are pertinent in relation to the proposed policy and would require further discussion:

    a) Should any further data protection obligations be included?
    For example, in Australia the Privacy Act provides for management of unsolicited messages; direct marketing, collection of solicited personal information, etc. However given that this intended policy is in relation to healthcare data, these aspects could potentially be taken up later in relation to a comprehensive data protection framework.

    b) How to address concerns in relation to information security of healthcare data?
    Data protection is closely associated with information security. Should the policy include certain standards that may be considered as "minimum compliance" or should the policy merely stipulate "maintaining information security" and leave it to the organisations/ data controllers to decide on how information is secured? Again it makes more sense to address these concerns at a later stage within a wider comprehensive data protection framework rather than a sector specific one.

Information not personally identifiable

58. It is crucial to deal with information that is no longer personally identifiable. **In many jurisdictions information that is not personally identifiable is not subject to the data protection regime.**

(VII) Disclosure of healthcare data for research

Pseudonymization and anonymization

59. Related to the notion of identifiability are the techniques of pseudonymization and anonymization. Pseudonymization refers to the technique of disguising identities, which ordinarily does not exclude data from the scope of personal data.[15] The EU GDPR recommends pseudonymization as a method of reducing risk to the data of individuals and as a method of meeting data protection obligations. It also prescribes technical and organisational safeguards in this regard.

60. Anonymization, by contrast, refers to data where all identifying elements have been eliminated from a set of personal data.[16] No element may be left in the information that could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data has been successfully anonymized, they are no longer considered to be personal data. **Anonymized data thus falls outside scope of data protection legislation in such systems**. Anonymization is a standard practice in various processes particularly in data aggregation. However, the extent of such anonymization is now a contested issue with instances emerging where individuals having been identified from supposedly anonymized data sets.

61. In the analyzed jurisdictions anonymized data is used for secondary purposes such as research. However, it is also increasingly common for a secure link or key to be retained so as to allow for such re-linking in certain predefined circumstances. This approach, variously referred to as "pseudonymization' or "reversible de-identification',[17] may be required to allow follow up quality control, or to verify, in the context of longitudinal research studies (where changes in data values over time are analysed), that temporally distinct datasets relate to the same patient.

62. In either case, (anonymization / pseudonymization) such de-identification processes do not provide a cast-iron guarantee to the patient of irrevocable privacy. This is because, even after removal of direct identifiers, there will usually be significant amounts of fairly specific information left over in the datasets - a series of medical data values, relating to the patient's health metrics, e.g. blood sugar level, blood pressure level, etc., plus the condition they are suffering from, and treatment episodes. Accordingly, it may remain possible for someone with access to the datasets to "match" the data with the same data available externally together with identifying information, e.g. on the Internet.[18] Indeed it is apparent that such possibilities are expanding daily, with the increasing power of data-mining techniques, and of search engines that allow combined search-term queries.

63. Given these risks, particularly of data-matching, various techniques have been tried in response. These include altering some of the values within individual de-identified

[15] White paper on data protection- India

[16] *Ibid*

[17] Such coding of patient data prior to secondary usage is mandated by international good practice research guidance: see e.g., the International Conference on Harmonization of Pharmaceutical Trials, Good Practice Guidelines, E6, R1, 2002, at [http://ichgcp.net/].

[18] W Lowrance, "Learning from Experience: Privacy and the Secondary Use of Data in Health Research', 2002, London: the Nuffield Trust; Report of the Academy of Medical Sciences, "Personal data for public good: using health information in medical research', London: 2006, at 12 ff; F Cate, "Protecting Privacy in Health Research: The Limits of Individual Choice' (2010) 98 *Cal LR*1765, at 1778 ff.

datasets (so-called "perturbation') as well as aggregating or merging datasets so that, rather than referring to individuals, they capture values simultaneously true of some minimum number of patients ("k-anonymity', etc.).[19] While such measures may make identification of individuals very difficult, they do not make it absolutely impossible. Moreover, there will almost always be a downside in terms of the reduced utility of the data in question - this is particularly true of suppressing chronological data, e.g. as to the date of treatment episode and observed outcome.[20] Broadly, the richer (and more potentially useful) data are in terms of allowing meaningful inferences, the greater the risk that those inferences may also include ones tending to the identification of the data subject.

64. The comparative positions of different jurisdictions in relation to the use of pseudonymized/ anonymized data/ information are outlined in the table below:

Legislation/ Jurisdiction	Provision	Comments
UK	Code of Anonymisation (under the Data Protection Act 1998). Anonymised data does not require compliance of data protection obligations.	The code explains the issues surrounding the anonymisation of personal data, and the disclosure of data once it has been anonymised. It explains the relevant legal concepts and tests in the Data Protection Act 1998 (DPA). The code provides good practice advice that will be relevant to all organisations that need to convert personal data into a form in which individuals are no longer identifiable. The term 'anonymised data' is used to refer to data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data. **The DPA does not require anonymisation to be completely risk free – one must be able to mitigate the risk of identification until it is remote**. If the risk of identification is reasonably likely the information should be regarded as personal data - these tests have been confirmed in binding case law from the High Court. Clearly, 100% anonymisation is the most desirable position, and in some cases this is possible, but the DPA does require it. The term 're-identification' is used to describe the process of turning anonymised data back into personal data through the use of data matching or similar techniques. <u>Disclosing anonymised data</u>

[19] See further H Greely, "The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks' (2007) 8 Annual Review of Genomics and Human Genetics 343; B Malin *et al,*"Technical and Policy Approaches to Balancing Patient Privacy and Data Sharing in Clinical and Translational Research' (2010) 58 *J. Investig. Med* 1. With pseudonymisation there is the additional risk that someone may make unauthorised use of the internal key to re-establish the patient's identity.

[20] Ibid.

Legislation/ Jurisdiction	Provision	Comments
		There is a clear legal provision that allows an organization to convert personal data into an anonymised form and disclose it, and once that is done, this will not be considered as a disclosure of personal data. This is the case even though the organisation disclosing the anonymised data still holds the original data that would allow re-identification to take place. This means that the DPA no longer applies to the disclosed data, therefore: • There is an obvious incentive for organisations that want to publish data to do so in an anonymised form; • It provides an incentive for researchers and others to use anonymised data as an alternative to personal data wherever this is possible; and • Individuals' identities are protected.
HIPAA (US)	De-identified data does not require approval for processing. Two methods are prescribed – Safe harbor and expert determination.	Direct identifiers are fields that can uniquely identify individuals, such as names, Social Security Numbers (SSN) and email addresses. In contrast, quasi-identifiers are fields that cannot immediately identify individuals but when linked with other identifiers increased the risk of individual re-identification exponentially. Examples of quasi-identifiers include dates, demographic information (such as race and ethnicity), and socioeconomic variables (occupation, salary). Safe harbor procedures allow organizations to disclose data without prior authorization, but stripped of 18 identifiers, 16 of which are classified as direct identifiers and include amongst others name, telephone number, and Social Security Number. The two quasi-identifiers are date and geography. Expert Determination method: It handles both direct and indirect identifiers. A statistician or person with appropriate training (expert) verifies that enough identifiers have been removed that the risk of identification of the individual is "very small." The Expert Determination method is a risk management exercise that incorporates both direct and quasi-identifiers. It satisfies both the need to protect the identity of individuals, while allowing organizations deep analysis on data used for secondary use.
GDPR	Qualified compliance for research purposes	Where an organisation can argue that the processing of health data is necessary for scientific research purposes, the GDPR provides a *qualified compliance framework* so long as safeguards are implemented. The appropriate safeguards include technical and organisational measures to ensure data minimization, i.e. processing the minimal amount of personal data.

Legislation/ Jurisdiction	Provision	Comments
		Pseudonymization is given as an example of the measures that could be used.
Australia	When information is appropriately de-identified it would not be subject to the application of privacy principles under the Privacy Act	A number of different terms are used in Australia to describe processes similar to de-identification, for example 'anonymisation' and 'confidentialisation'. In particular, 'confidentialisation' is used by the Australian Bureau of Statistics (ABS) There is no specific process for de-identification. However, removal of direct identifiers alone is deemed insufficient. De-identification generally involves two steps. First removal of direct identifiers and secondly taking one or both of the following steps: • Removing or altering other information that may allow an individual to be identified (for example, because of a rare characteristic of the individual or a combination of unique or remarkable characteristics that enable identification), And/ Or • Putting controls and safeguards in place in the data access environment, which will appropriately manage the risk of re-identification.
Singapore	Guide to basic anonymisation techniques	It lays down the various techniques for anonymisation without recommending any particular one, like attribute suppression, record suppression, character masking, pseudonymisation, swapping, replacement, data suppression, data recoding / generalization, data shuffling and masking.
India	The Draft data protection legislation does not apply to anonymized data	"Anonymisation" in relation to personal data, means the "irreversible process" of transforming or converting personal data to a form in which a data owner cannot be identified, meeting the standards specified. The code in relation to anonymisation has not yet been published.

Proposed framework for processing data for research purposes in Sri Lanka

65. Based on the proposed DISHA Act of India, it is suggested that in the context of Sri Lanka, healthcare data be allowed to be processed for research and improved service delivery, and for the following purposes:[21]

[21] DISHA have been used as the basis for adoption in the Sri Lanka context for several reasons: (a) use of simple language that leaves limited room for misinterpretation; (b) it encompasses the various "use cases" including purposes like research, prevention of diseases etc.; (c) the proposed provision clearly delineates between personally

a) To advance the delivery o**f patient centered medical care;**

b) To provide appropriate information to **help guide medical decisions at the time and place of treatment;**

c) To improve the coordination of **care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data;**

d) To improve **public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks;**

e) To facilitate **health and clinical research and health care** quality;

f) To promote **early detection, prevention, and management of chronic diseases;**

g) To carry out **public health research, review and analysis, and policy formulation;**

h) To undertak**e academic research and other related purposes;**

66. Furthermore, processing for the above outline purposes, be only be under the condition that **personally identifiable information may only be used for the purposes of direct care of the owner of the data,** to the extent considered necessary, and in the best interest of the owner.

67. Furthermore, processing for the purposes mentioned in Paragraph 65(d) to 65(h), **only de-identified or anonymized data shall be used, in the manner as may be prescribed under the final policy.**

- In the first instance, Sri Lanka may consider the wholesale adoption of HIPAA's Safe Harbor rules, with appropriate modifications.
- However it will be important for Sri Lanka to build the necessary legal and institutional mechanisms as well as the technical capacity to reduce the risk of re-identification. This would mean that eventually Sri Lanka should have a viable Expert Determination approach (similar to what is outlined under HIPAA). As such working group(s) should be formulated to study the sate of the art in statistical techniques to mask identity as well as related technologies as may be needed when disclosing data for research purposes. Here to in the initial states, adoption (with appropriate modification) of approaches utilized in other jurisdictions like the US or Singapore (the latter in particular also allows for mandatory disclosure under strict conditions and with additional obligations on the receiver),[22] may be appropriate.

identifiable data and de-identified / anonymized data. The language employed provides paramount protection to patient data.

[22] See table in Paragraph 69

(VIII) Mandatory Disclosure

68. Mandatory disclosure refers to the disclosure of healthcare data without consent. It is understood that in certain exceptional circumstances personal data is required to be disclosed even without obtaining the consent of the data owner. The section on mandatory disclosures relates to those exceptional instances where personally identifiable (not anonymized, pseudonymized, or de-identified) data is required to be disclosed although no consent has been obtained from data owner.

Existing Sri Lankan context

69. Several existing Sri Lankan legislations outline specific contexts under which mandatory disclosure is required.

    a) The Contagious Diseases Ordinance imposes a duty to report about smallpox, cholera etc.[23]

    b) National Medicines Regulatory Authority Act requires authority to furnish information to the Minister under Minister's direction (wide powers vested with the Minister).[24]

Comparative Positions

70. The table below outlines the comparative positions in different jurisdictions in relation to mandatory disclosure

Legislation/ Jurisdiction	Provision	Comments
UK	Mandatory disclosures under various legislations including *The Health and Social Care (Safety and Quality) Act 2015;* *Health Protection (Notification) Regulations 2010; Abortion Regulations 1991; Reporting of Injuries, Diseases and*	There are also exceptional circumstances in which a health or social care professional may be obliged to share confidential patient information in line with the 'public interest'. Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and

[23] Contagious Diseases Ordinance – Section 3: Every householder residing in Sri Lanka shall be bound to report, with the least possible delay, to the Superintendent of Police, or to some inspector of police, or to some police constable or grama niladhari of his town or village, every case occurring in the house in which he resides of smallpox, cholera or other disease which may, from time to time, be named by the Minister in an Order to be by him for that purpose issued, and any householder neglecting to make such report shall be liable on conviction thereof to a fine not exceeding twenty rupees; and every inspector of police, police constable, or grama niladhari to whom any such case shall be reported by such householder, or by any other person, or who shall know of the existence of any such case within such town or village, shall forthwith report the same to the Superintendent of Police or to some Magistrate within the district in which such town or village is situated.

[24] National Medicines Regulatory Authority Act - Section 26 (2): The Minister may direct the Authority to furnish to him in such form as he may require, returns, accounts and any other information relating to the work of the Authority, and it shall be the duty of the Authority to give effect to such directions.

Legislation/ Jurisdiction	Provision	Comments
	Dangerous Occurrences Regulations 2013; Female Genital Mutilation Act 2003	imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime.
HIPAA (US)	Disclosure of PHI without "authorization" subject to "waiver of authorization" by Institutional Review Boards (IRBs) or Privacy Boards subject to fulfillment of conditions. Conditions include minimal risk to breaching privacy of individuals b) adequate plan to protect identifier c) adequate plan to destroy identifiers d) adequate assurances that PHI will not be reused e) research could not be practically conducted without the waiver or access to PHI.	An IRB or a Privacy Board may waive the authorization requirement in whole or in part. A complete waiver of authorization means that no authorization is required for the covered entity to use and disclose PHI. A partial waiver means that the IRB or Privacy Board determined that a covered entity does not need authorization for the uses and disclosure of the PHI for one part of a research project, but does need to obtain authorization from patients for another part of the project.
India	Chapter IX of the Draft Data Protection Act deals with exemptions.	The exemptions can relation to security of state, prevention; investigation and prosecution for contravention of law; processing for legal proceedings; research, archiving or statistical purposes; journalistic purposes; manual processing by small entities.
Singapore	Schedule of PDPA	Use of personal information is permitted without consent if such use is for *inter alia*[25] - necessary for any purpose *which is clearly in the interests of the individual*, - if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent; - the use is necessary to respond to an *emergency* that threatens the life, health or safety of the individual or another individual; - the use is necessary for *evaluative purposes*; - For *research purposes* (only under specific instances, but also with additional obligations on the receiving party)

[25] Please refer to the complete PDPA 2012 act at https://sso.agc.gov.sg/Act/PDPA2012

Legislation/ Jurisdiction	Provision	Comments
Australia	There are exceptions to the application of privacy principles for "permitted health situation" or "permitted general situation".	"permitted heath situation" applies when: *Collection* of health information to provide a *health service* or for certain *research and other purposes* *Use or disclosure* of health information for certain research or other purposes of genetic information to lessen or prevent a serious threat to the life, health or safety of a genetic relative of the patient The disclosure of health information to a responsible person for a patient "permitted general situation" there are seven under this category the most relevant for health data is - where it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure of their health information, and it can be reasonably believed that it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety

Mandatory disclosure for research purposes

71. As discussed above HIPAA provides for mandatory disclosure under strict grounds on a case-by-case basis. GDPR on the other hand only allows for a qualified compliance framework (outlined earlier in Paragraph 64)

72. As can be seen from the table above under Paragraph 70, the different jurisdictions do allow for the processing of anonymized / pseudonymized data for varied purposes including research and in the case of Singapore also for the disclosure of personal data under strict pre-conditions, and with additional obligations on the receiver of the data.

Items for further discussion

73. The Code for Conduct of Human Research in Sri Lanka published in April 2018 provides for elaborate standards in relation to the conduct of research. However to date, Sri Lanka does not have any specific provision for **disclosure without consent for research purposes**. Should healthcare data along with personally identifiable information (where consent of the data owner has not be obtained) be made available for research purposes and if so under what conditions?

(IX) Additional areas for discussion

Measures required to ensure information security

74. Information security is a critical issue and has been subject to scrutiny in several jurisdictions. The Singapore health data breach of mid 2018 attracted widespread attention, as up until that time, the security flaws were undetected.

75. Sri Lanka CERT has certain information security guidelines for public authorities, based on ISO standards, which could be a possible starting point.

Enforcement of policies and penalties for non- compliance

76. The policy does not encompass any mechanism to ensure enforcement and / or consequences of non-compliance. To ensure that the enshrined data protection obligations are complied with and transgressions penalized it is essential to establish a regulatory regime that includes penalties and related procedures.

Subsequent guidelines (the committees formed under the National Policy on Health Information)

77. Under the National Health Information Policy 4.1 it is required that the DGHS, DDG(ET&R),DDG(P) establish guidelines 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. Further, the D/HI, DDG(P) are required to establish guidelines and integral mechanisms in health information sub-systems to ensure controlled access to individually identifiable data/information and health data
78. The access control shall be role based and decided on a need to know and need to do basis.

79. A time of 24 months has been given in this regard. Once these guidelines are formulated, it will lead to better clarity.

Guidelines for “primary business” and a committee for issues arising thereon

80. It is essential to lay down guidelines as to what denotes “primary business” of providing healthcare. This is crucial to defining the scope of the proposed policy. It is deemed fit that these guidelines should not be exhaustive and should allow for determination by an expert committee in instances of dispute / ambiguity.