Internship Training

at

National Institute of Health and Family Welfare, New Delhi

(Feb 20, 2018- May 10, 2017)

A study on

Study of Cyber Security Framework for Healthcare in India

By

Name: Col Sanjeev Kumar Ahluwalia

Enrollment No.: PG/16/052

Under the guidance of

Dr. S.N. Sarbadhikari

Post-graduate Diploma in Hospital and Health Management
2016-2018

International Institute of Health Management Research, New Delhi

Internship Training

at

National Institute of Health and Family Welfare, New Delhi

(Feb 20, 2018- May 10, 2017)

A study on

Study of Cyber Security Framework for Healthcare in India

By

Name: Col Sanjeev Kumar Ahluwalia

Enrollment No.: PG/16/052

Under the guidance of

Dr. S.N. Sarbadhikari

Post-graduate Diploma in Hospital and Health Management
2016-2018

International Institute of Health Management Research, New Delhi

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Col Sanjeev Kumar Ahluwalia, student of Post Graduate Diploma in Hospital and Health Management (PGDHM) from International Institute of Health Management Research, New Delhi has undergone internship training at National Institute of Health and Family Welfare, New Delhi from Feb 20, 2018 to May 10, 2018.

The Candidate has successfully carried out the study designated to him during internship training and his approach to the study has been sincere, scientific and analytical.

The Internship is in fulfillment of the course requirements.

I wish him all success in all his future endeavors.

Dr Supten Sarbadhikari
Dean, Academics and Student Affairs
IIHMR, New Delhi

Mentor

IIHMR, New Delhi

(Completion of Dissertation from respective organization)

The certificate is awarded to

Name: Col Sanjeev Kumar Ahluwalia

in recognition of having successfully completed his
Internship in the department of

Centre for Health Informatics,

and has successfully completed his Project on

Study of Cyber Security Framework for Healthcare in India

Date: May 10, 2018

Organisation: National Institute of Health and Family Welfare, New Delhi

He comes across as a committed, sincere & diligent person who has

a strong drive & zeal for learning

We wish him all the best for future endeavors

Training & Development **Zonal Head-Human Resources**

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled **"Study of Cyber Security Framework for Healthcare in India"** and submitted by **Col Sanjeev Kumar Ahluwalia,** Enrollment No. **PG/16/52** under the supervision of **Dr. S.N. Sarbadhikari, Dean, Academics and Student Affairs, IIHMR, New Delhi and Mr. Ankit Tripathi, Additional Director, NIHFW, New Delhi** for award of Postgraduate Diploma in Hospital and Health Management of the Institute carried out during the period from Feb 2018 to May 2018 embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other Institute or other similar institution of higher learning.

Signature

CERTIFICATE OF APPROVAL

The Summer Training Project titled **"Study of Cyber Security Framework for Healthcare in India"** at **"**National Institute of Health and Family Welfare (NIHFW)**"** is hereby approved as a certified study in management carried out and presented in a manner satisfactorily to warrant its acceptance as a prerequisite for the award of **Post Graduate Diploma in Health and Hospital Management** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the report only for the purpose it is submitted.

Dr. S.N. Sarbadhikari

IIHMR, Delhi

CERTIFICATE FROM DISSERTATION ADVISORY COMMITTEE

This is to certify that **Col Sanjeev Kumar Ahluwalia,** a graduate student of the **Post-Graduate Diploma in Health and Hospital Management** has worked under our guidance and supervision. He is submitting this dissertation titled "**Study of Cyber Security Framework for Healthcare in India**" at "National Institute of Health and Family Welfare" in partial fulfillment of the requirements for the award of the **Post-Graduate Diploma in Health and Hospital Management.**

This dissertation has the requisite standard and to the best of our knowledge no part of it has been reproduced from any other dissertation, monograph, report or book.

Dr. S.N. Sarbadhikari
Dean, Academics and Student Affairs

IIHMR, Delhi

Mr. Ankit Tripathi
Additional Director

Centre for Health Informatics
National Institute of Health and Family Welfare, New Delhi

CERTIFICATE OF APPROVAL

The following dissertation titled **"Study of Cyber Security Framework for Healthcare in India"** at **"National Institute of Health and Family Welfare"** is hereby approved as a certified study in management carried out and presented in a manner satisfactorily to warrant its acceptance as a prerequisite for the award of **Post Graduate Diploma in Health and Hospital Management** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the dissertation only for the purpose it is submitted.

Dissertation Examination Committee for evaluation of dissertation.

Name	Signature
_____	_____
_____	_____
_____	_____

FEEDBACK FORM

Name of the Student: Col Sanjeev Kumar Ahluwalia

Summer Training Institution: Centre for Health Informatics / National Institute of Health and Family Welfare, New Delhi

Area of Summer Training: Comparative Study of Regulations for Cyber Security of Healthcare in India

Attendance:

Objectives met:

Deliverables:

Strengths:

Suggestions for Improvement:

Signature of the Officer-in-Charge/ Organisation Mentor (Dissertation)

Date:
Place:

ABSTRACT

Background Information Technology (IT) has become integral part of all aspects of life and healthcare is no exception. The advantages of IT are well known: efficient storage, easy retrieval, high speed of processing, without error or bias, improving efficiency. Health records contain important information of patients, thus, the ability of healthcare professionals to access them at the requisite time and place can ensure positive outcomes.

Data gathered by the healthcare providers for the benefit of patients are also targeted by cyber criminals for intentional disruption, data ransoming, corporate espionage, and financial crimes. These cyber threats can lead to situations which may impact patient care and public health as was done with the recent “ransomware” incident that struck hospitals and other systems across the globe.

The healthcare providers and government take these threats very seriously in light of the fact that privacy has been declared as fundamental right by the Hon’ble Supreme Court. Two areas needs attention: protection of healthcare related data and government IT systems. This requires coordination amongst all stakeholders, including private sector, to help protect their IT systems.

Aim To study cyber security issues related to healthcare, analyse gaps and formulate draft cyber security policy or guidelines for healthcare.

Type of Study Descriptive/Qualitative

Design A study of 9 national / International papers / Acts, standards and guidelines was carried out.

Findings Gaps in Draft "Digital Information Security In Healthcare, Act (DISHA)" of MoHFW, No Computer Emergency Response Team- Health (CERT-H), No Cyber Security Audit and No formalised training / awareness of employees on Cyber Security aspects.

Recommendations Formulation of Cyber Security Cell; Periodic Cyber Audit; Awareness training**;** Comments / gap analysis of Draft "Digital Information Security In Healthcare, Act (DISHA)" of MoHFW , draft Cyber Security Policy for Healthcare.

ACKNOWLEDGEMENT

I take this opportunity to express my gratitude to everyone who supported me throughout the course of my PGDHM summer internship project. I am thankful for their aspiring guidance, invaluably constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project.

I am highly obliged to Mr. Ankit Tripathi, Additional Director, Centre for Health Informatics (CHI) for allowing me to pursue my Summer Training from National Institute of Health and Family Welfare (NIHFW), New Delhi. I would sincerely like to thank him for his immense guidance and constant training in providing necessary information regarding the project despite his preoccupation and busy schedule.

I would also like to express my gratitude towards Mr. Manpreet Singh, Consultant CHI, New Delhi for being helpful and guiding me throughout my training.

I would like to like to express my sincere thanks to Dr. Sanjay Gupta, Dean NIHFW, New Delhi without whom this project would have been a distant reality.

I feel privileged to express my heartfelt gratitude and deep appreciation to my esteemed Professor and Mentor Dr. S.N. Sarbadhikari without whom this project would have been a distant reality. His tireless pursuit for perfection and professional approach were constant inspiration for me. He advised me to study “White Paper of the Committee of Experts on a Data Protection Framework for India” and draft “Digital Information Security In Healthcare (DISHA) Act”. In hindsight, I realize that without these papers the study would have been incomplete.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

MoHFW	Ministry of Health and Family Welfare
NIHFW	National Institute of Health and Family Welfare
CHI	Centre for Health Informatics
ISO	International Organization for Standardization
NDHA	National Digital Health Authority
CERT-H	Computer Emergency Response Team-Health
MS	Medical Superintendent
HR	Human Resource
AMS	Assistant Medical Superintendent
HIS	Hospital Information System
AMC	Annual Maintenance Contract
NABL	National Accreditation Board for Testing And Calibration Of Laboratories
TQM	Total Quality Management
ICU	Intensive Care Unit
SDPI, Rules	Sensitive Personal Data or Information Rules 2011

LIST OF APPENDICES

PART 1: OBSERVATIONAL LEARNING

INTRODUCTION: NIHFW

1. The National Institute of Health and Family Welfare (NIHFW), was established on 9th March, 1977 by the merger of two national level institutions, viz. the National Institute of Health Administration and Education (NIHAE) and the National Institute of Family Planning (NIFP). The NIHFW, an autonomous organization, under the Ministry of Health and Family Welfare, Government of India, acts as an 'apex technical institute' as well as a 'think tank' for the promotion of health and family welfare programmes in the country.

The Institute addresses a wide range of issues on health and family welfare from a variety of perspectives through the departments of Communication, Community Health Administration, Education and Training, Epidemiology, Management Sciences, Medical Care and Hospital Administration, Population Genetics and Human Development, Planning and Evaluation, Reproductive Bio-Medicine, Statistics and Demography and Social Sciences.

VISION & MISSION

2.1 VISION

NIHFW is to be seen as an Institute of global repute in public health & family welfare management.

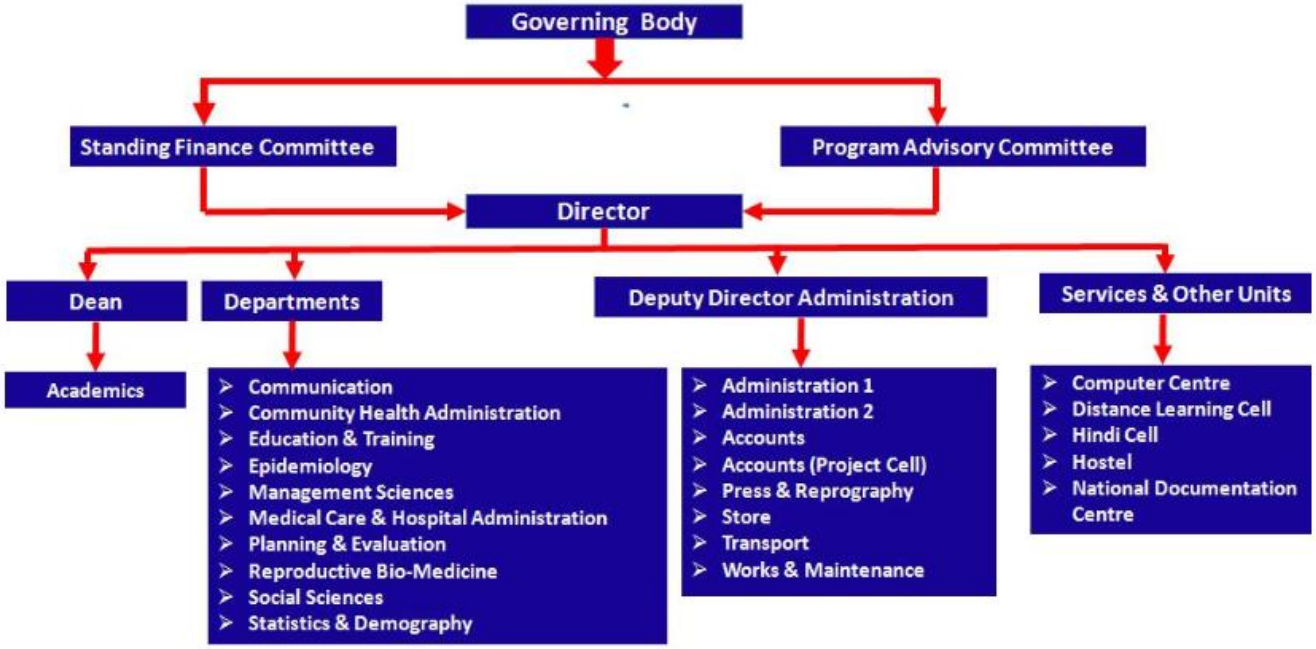
2.2 MISSION

To act as think tank, catalyst & innovator for management of public health and related health & family welfare programmes by pursuing multiple functions of Education & Training, Research & Evaluation, Consultancy & Advisory services as well as provision of specialised services through inter-disciplinary teams.

ORGANISATION

3. The Governing Body GB) is the apex policy making body for NIHFW. It comprises of Minister of Health and Family Welfare, Government of India, New Delhi (Chairman) ; Secretary (FW), Ministry of Health and Family Welfare, Government of

India, New Delhi (Vice-Chairman); Additional Secretary (Health), Ministry of Health and Family Welfare, Government of India, New Delhi (Member); Director General of Health Services, Government of India, New Delhi (Member); Addl. Secretary (Dealing with NIHFW), Ministry of Health and Family Welfare, Government of India, New Delhi (Member); Addl. Secretary (Financial Advisor), Ministry of Health and Family Welfare, Government of India, New Delhi (Member); Director General, Indian Council of Medical Research, Ansari Nagar, New Delhi (Member); Director , All India Institute of Medical Sciences, Ansari Nagar, New Delhi (Member); Director, International Institute for Population Sciences, Govandi Station Road, Deonar, Mumbai (Member); seven members to be nominated by Chairman; Director, National Institute of Health and Family Welfare, Munirka, New Delhi acts as member-Secretary.



FACILITIES

4.1 RBM Clinic: Antenatal care (screening, problem identification and appropriate action including referral), Immunisation, Contraceptive services, Management of infertile couples, Management of reproductive endocrinological disorders.

4.2 Demographic Data Centre

4.3 Computer Centre

4.4 Video Conferencing

4.5 Hostel

4.6 Centre for Health Informatics (CHI)

(i) General Objectives

- The Project aims to improve the health literacy of the masses in India.
- It aims to improve access to health services across the nation.
- It aims to decrease the burden of disease by educating the people on the preventive aspects of disease.

(ii) Specific Objectives

- Improve access to services through IT enabled cataloguing of service providers.
- Create a comprehensive web based National Health Portal to make available comprehensive health related information to the community using IT and analogue or Non-IT methods.
- Create protocols to enable the masses to access reliable, easy to understand, multilingual health information from the interactive National Health Portal.
- Create protocols for wide dissemination of health information in public domain using the Internet and other pertinent communication modalities.
- Create databases to enable citizens to seek, locate and access health care providers across the country.
- Create platforms to provide health information and health resources for the healthcare workers, NGOs, student communities, and health professionals.
- Create a transparent resource on regulatory and statutory guidelines pertaining to healthcare in India.

PROJECT REPORT: STUDY OF CYBER SECURITY FRAMEWORK FOR HEALTHCARE IN INDIA

1. Introduction

1.1 Background

The digital world is a reality today and Information Technology (IT) has become integral part of our life, including healthcare. The advantages of IT are well known: efficient storage, easy retrieval, high speed of processing, without error or bias, improving efficiency. Health records contain important information of patients, thus, the ability of healthcare professionals to access them at the requisite time and place can ensure positive outcomes.

Traditionally, information available in healthcare facilities has been safely managed by keeping it in paper records throughout its lifecycle i.e. creation, storage, access, modification, distribution, and destruction. However, to make all healthcare services accessible to service providers and the people, the government has steadily graduated towards using electronic formats of information. Now, several forms of information have been converted to the electronic format by the ministries, departments and agencies, both in the central as well as state governments. The classification, storage and protection of such information in electronic format have always remained an area of concern. The challenge, as with the information contained in paper format, remains the same, namely the ability to categorize, protect, archive, discover, and attribute information during its useful life and eventual destruction. Even though the lifecycle of information remains the same in electronic documents and online transactions, the methods to secure information in electronic environment are different.

As the government and private sector healthcare providers broadens the scope of their efforts to move towards e-governance and embrace technology for citizen-centric services, it faces threats from multiple sources. Each government process or project introduces a different level of complexity as a result of varied data transactions, involvement of multiple players and exposure to increasing compliance requirements. This complexity is applicable for both government and private sector, even though private sector healthcare providers are early adopters of technology and innovation. Such complexity associated with the lifecycle of information poses serious challenges in managing and governing security and ensuring compliance. Thus, it is essential to establish a practical policy initiative for the security of information and to sensitize public and private sector towards cyber security concerns. This will instill trust in IT services provided by the government and private agencies and thus will help further expand in improved e-governance services to various stakeholders.

Cyber security has many challenges which are generally not very prominent in conventional physical security, like: these threats may come from across the national boundaries; the identity of the attacker and the source is difficult to ascertain; difficult to

collect irrefutable evidence against a cyber-attacker. Thus it's very essential that healthcare providers take adequate precautions and use best Information security practices involving latest technology and adequate controls.

1.2 Reasons for Taking up the Study **There is no cyber security policy for healthcare with MoHFW.**

1.3 Problem Statement: The Ministry of Health and Family Welfare (MoHFW) is the process of establishing Integrated Health Information Platform (IHIP) for integrating health related data networks of different hospitals and various agencies. Security of this network will be of paramount important due to the fact that different hospitals (government and private), various agencies (government departments, insurance companies) and different institutions (Medical Colleges, Research institutes) will be sharing protected health information on this network. However, presently there is no formal cyber security policy for healthcare.

2. Literature Review

2.1 White Paper of "The Committee of Experts on A Data Protection Framework For India", Justice B.N. Srikrishna Committee

The Government of India has set up our Committee of Experts to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill.

2.2 Draft "Digital Information Security In Healthcare, Act (DISHA)"

Draft "Digital Information Security In Healthcare, Act (DISHA)" was put in public domain by Ministry of Health and Family Welfare (MoHFW) on March 21, 2018 and comments were sought by April 21, 2018.

2.3 IT Act 2000.

2.4 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. (SPDI)

2.5 EHR Standards 2016 of MoHFW.

2.6 ISO 27001: Information Technology – Security Technique- Information Management System-Requirements.

2.7 ISO 17799: Information Technology – Security Technique- Code of Practice for Information Security Management.

2.8 National Cyber Security Policy 2013, Department of Electronics and Information Technology.

2.9 Health Insurance Portability and Accountability Act (HIPAA) of 1996, United States.

3. Objective & Scope

3.1 **Objective** To study cyber security issues related to healthcare, analyse gaps and formulate draft cyber security policy or guidelines for healthcare.

3.2 **Scope**

3.2.1 Study the existing and proposed IT system for healthcare.

3.2.2 Study cyber security policy and guidelines of Government of India, Ministry of Electronics and Information Technology.

3.2.3 Study existing instructions/ letters/ literature regarding cyber security for healthcare.

3.2.4 Assess gap in current / proposed systems.

3.2.5 Formulate draft Cyber Security Policy for healthcare.

3.2.6 Recommend organisation for Cyber Security Cell and CERT-H .

3.2.7 Recommend Cyber Security Awareness Training.

3.2.8 Recommend evaluation / Audit of Healthcare IT System.

4. Methodology

4.1 Type of Study : Descriptive / Qualitative and Observational Study of Physical Security aspects.

4.2 Location of Study : National Institute of Health and Family Welfare.

4.3 Study Area : Cyber Security in healthcare.

4.4 Study Design : A study of 9 national / International papers / Acts, standards and guidelines was carried out.

4.5 Analysis : Gap analysis of the existing / proposed Cyber Security framework was analysed for requirement and risks involved in Healthcare.

5. Findings

5.1 White Paper of "The Committee of Experts on A Data Protection Framework For India", headed by Justice B.N. Srikrishna is very comprehensive paper and cover all aspects and framework required for "Data Protection Law in India". Summary of issues discussed in the White Paper are given at Appendix A.

5.2 Gaps Observed in Draft "Digital Information Security In Healthcare (Disha) Act"

Draft "Digital Information Security In Healthcare, Act (DISHA)" was put in public domain by Ministry of Health and Family Welfare (MoHFW) on March 21, 2018 and comments were sought by` April 21, 2018. Following gaps were observed in the Draft Act:

5.2.1 Nomenclature: NDHA vs NeHA As per the MoHFW covering letter dt 21 Mar 2018 regarding comments on the draft Act, National Digital Health Authority (NDHA) is proposed to be set up, however, as per Section 4, Chapter II of the proposed Act National Electronic Health Authority (NeHA) shall be established.

5.2.2 Para 3(1)(c): Consent As per IT Act 2000, any electronic document which is not digitally signed is equivalent to unsigned paper document. However, Consent (in physical or paper form) has to be signed by an individual.

5.2.3 Para 3(1)(c): 'Digital Health Data' The heath data given is not complete.

5.2.4 Para 3(1)(k): 'Personally Identifiable Information' "Protected Health Information" will be more suitable instead of 'Personally Identifiable Information'.

5.2.5 Para 3(1)(n): 'Data Security' Data related to Protected Health Information (PHI) needs to be secured and not only the Digital Health Data which is subset of the PHI.

5.2.6 Para 3(1)(o): 'Sensitive Health Related Information"

This is little confusing as a term 'Digital Health Data' has also been mentioned at Section 3(1)(c).

5.2.7 Section 28(1): The rights of the owner of digital health data

The owner of the heath data has the right to privacy and a Clinical Establishment has to implement it by ensuring security of this data. The paragraph needs amendment.

5.2.8 Section 28(2): The rights of the owner of digital health data

This section contradicts the provisions of Section 29 of the Act.

5.2.9 Section 28(3) and Section 28(4): The rights of the owner of digital health data

An individual's right should be limited to give consent to share his/her information along with individually identifiable information or not.

5.2.10 Section 41, 42: Obtaining Digital Health Information of another Person & Data Theft

Similar such crimes i.e. data theft and fraudulently obtaining data, are covered under IT Act 2000, so provisions of IT Act 2000 should be made applicable otherwise there can be confusion if punishments are not same in both the Acts.

5.3 It was noticed that MoHFW didn't have Cyber Security Cell which is essential to ensure adherence to Cyber Security policies by all stakeholders. in case of large scale. However, it is now learnt that steps to formulation of Cyber Security Cell have been initiated. Though Computer Emergency Response Team-Health (CERT-H) has not been formulated which should be responsible to deal with the large scale failure of Health IT Systems due to intentional or unintentional reasons.

5.4 There is no Cyber Security Policy of the MoHFW.

5.5 There is formal system of Cyber Security audit by the MoHFW.

5.6 There is no established system for improving the awareness of employees regarding Cyber Security issues in Healthcare.

5.7 Physical Security Aspects Observed at MoHFW

5.7.1 Entry to offices is well regulated.

5.7.2 System for access to offices is well established and is strictly adhered to.

5.7.3 Installation of biometric systems to every office will enhance security.

5.7.4 Installation of CCTV cameras in the corridors will further improve the security and will act as deterrence for wrongdoings.

6. Recommendations

Ser No.	DISHA / Other Cyber Security Aspects	Recommendations (As per Justice B.N. Srikrishna Committee, ISO 27001 / ISO 17799/ IT Act 2000/ HIPAA
6.1	Cyber Security Policy not formulated	As per ISO 17799, "An information security policy document should be approved by management, and published andcommunicated to all employees and relevant external parties".

		MoHFW should formulate Cyber Security poicy. Draft Cyber Security Policy is given at Appendix B.
6.2	No formal Cyber audit	As per White Paper, Data Protection Impact Assessment and Audit should be carried out. As per ISO 17799, Information Systems should be regularly checked for Security Policy, Standards and Technical Compliance. . Inter Audit – Every Quarter. External Audit – Annually.
6.3	No CERT-H nominated	CERT-H be established to handle large scale disruption of IT Systems or major cyber security issues
6.4	No formal training	As per ISO 17799, cyber security awareness be carried for all employees Training be planned for all employee, including for senior management.
6.5	NDHA vs NeHA (Draft DISHA)	As per the MoHFW covering letter dt 21 Mar 2018 regarding comments on the draft Act, National Digital Health Authority (NDHA) is proposed to be set up, however, as per Section 4, Chapter II of the proposed Act National Electronic Health Authority (NeHA) shall be established. NeHA is broader term, may be considered.
6.6	Consent in written or Electronic form (Draft DISHA:Para 3(1)(c))	As per IT Act 2000, an electronic document not digitally signed is equivalent to unsigned paper document. Electronic consent be signed using digital signature or Aadhar.
6.7	Digital Health Data (Draft DISHA:Para 3(1)(e))	Following may be added to Digital Health Data: i. EMR/EHR. ii. Lab reports. iii. Radiographic reports. iv. Medicines consumed while admitted in a hospital/ prescribed by a doctor. v. Payment made to the healthcare provider by an individual directly or through Health Insurance Company.
6.8	Personally Identifiable Information (Draft DISHA:Para 3(1)(k)	Protected Health Information It is recommended that instead of 'Personally Identifiable Information', 'Protected Health Information' may be used, as it is more relevant in the present case. And following details may be included for 'Personally Identifiable Information' or 'Protected Health Information' in Schedule I : i. Name. ii. Geographical identifiers smaller than a state i. e.

		District and below. iii. Dates (other than year) directly related to an individual. iv. Phone/ FAX Numbers. v. Email addresses. vi. Medical record numbers. vii. Health insurance beneficiary numbers. viii. Bank Account numbers/Debit/Credit Card details. ix. License numbers. x. Vehicle identifiers i.e. RC numbers. xi. Web Uniform Resource Locators (URLs) and Internet Protocol (IP) address numbers. xii. Biometric identifiers, including finger, retinal and voice prints. xiii. Full face photographic images and any comparable images. xiv. Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL'). xv. Any other unique identifying number.
6.9	Data Security (Draft DISHA:Para 3(1)(n)) .	Paragraph may be amended as below **'Data Security'** refers directly to "Protected Health Information (PHI)", and specifically to the means used to protect the privacy of health information contained in digital health data that supports professionals in holding that information in confidence.
6.10	'Sensitive Health Related Information" (Draft DISHA:Para 3(1)(o))	As per Sensitive Personal Data or Information Rules, 2011 and HIPAA, all data related to health should be considered as sensitive, however this paragraph is giving an impression as if only some data related health is sensitive and not the complete health data. Complete data related to health be treated as sensitive.
6.11	The rights of the owner of digital health data (Draft DISHA:Section 28(1))	As per HIPAA, the owner of the heath data has the right to privacy and a Clinical Establishment has to implement it by ensuring security of this data. The paragraph may be amended as under: An owner shall have the right to privacy of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.
6.12	The rights of the owner of digital	Electronic Health data is an equivalent of physical records being maintained by clinical establishments and these are

	health data (Draft DISHA: Section 28(2))	required, thus, no consent should be essential for maintaining legitimate medical records. In fact it is mandatory to maintain medical records for medico legal cases. Thus this section should be amended as Clinical Establishment needs to collect and store health data for provision of requisite healthcare services and for future use for benefit of an individual. An individual should be given right to give consent to share his/her information along with individually identifiable information or not, like for research Health data should be collected and stored for at least for 3 years or as per policy in secured manner.
6.13	The rights of the owner of digital health data (Draft DISHA: Section 28(3) and Section 28(4))	An individual's right should be limited to give consent to share his/her information along with individually identifiable information or not.
6.14	Obtaining Digital Health Information of another Person & Data Theft. (Draft DISHA: Section 41, 42)	Crimes similar to as mentioned in these sections e.g. Data Theft; Fraudulently obtaining Data, are covered under IT Act 2000 also. Provisions of IT Act 2000 should be made applicable for such crimes otherwise there may be confusion if punishments are not same in both the Acts.

6.15 **<u>Cyber Security Policy</u>** MoHFW should formulate Cyber Security Policy considering existing and standards: (a) Cyber Crisis Management Plan issued by Ministry of Communication and Information Technology; (b) ISO 271000; (c) ISO 17799

<u>Cyber Security Policy for Healthcare</u>

Cyber Security Policy is an important document for all organisations using Information Systems. All organisations must prepare their own Cyber Security Policy considering following aspects:

(a) Vision, Mission and Objectives of organisation.

(b) Existing and proposed Information Systems in the organisation.

(c) Risk Assessment.

(d) Risk Acceptance

(e) Risk Assessment needs to be conducted a number of times so that all relevant issues are considered.

(f) Scope of a risk assessment should be clearly defined, like whole organization or parts of the organization, an individual information system, specific system components, or services.

(g) Risk assessment activity should also be carried out periodically, may after every 3 years, to address changes in the security requirements and in the risks based on threats and vulnerabilities.

(h) Treatment of Risks:

(i) Technical solutions to avoid security risks.

(ii) Technical Standards as per national and international/national legislation and regulations;

(iii) Management Actions

(iv) Priority for managing security risks.

(vi) Management and procedural Controls to prevent security risks.

(j) Thus every organisation must review their Cyber Security Policy every 3 years or in case of any major changes in the Information Systems or major security vulnerability found in the existing system.

A draft Cyber Security Policy for Healthcare, considering above mentioned aspects, has been formulated and is given at Appendix B.

6.16 Computer Emergency Response Team-Health (CERT-H) be formulated to deal with unforeseen emergency situations. Recommended composition of the Committee is as under:

(a)	Secretary, MOHFW	-	Chairman.
(b)	Additional Secretary,eHealth	-	Member.
(c)	Chief Information Security Officer, MoHFW	-	Member.
(d)	Representative from CERT-In	-	Member .
(e)	HoD Computer Science Deptt, IIT,New Delhi	-	Member.
(f)	Additional Director, CHI, New Delhi	-	Member.
(g)	Three Cyber Security Experts from Industry	-	Member.

6.17 <u>Cyber Security Audit</u> It is recommended that

(a) A quarterly Internal Cyber Security Audit be carried out by all organizations.

(b) Annual Cyber Security be carried out through certified External agency.

6.18 **Awareness / Education of Employees** A formalized training is recommended as under:

(a) All employees should be made aware about Cyber Security issues. For new employees, this aspect may be included in the Induction Training.

(b) For employees working in the IT System, a training cadre be organized every year from an external agency.

(c) For Senior Managers, awareness training / talk be organized once in two years preferably by external agency.

7. Limitations of the Study

7.1 Due to the paucity of time Cyber Security framework of developed nations could not be carried out.

7.2 Due to paucity of time and due to procedural issues, Cyber Security audit / check of hospitals / organizations could not be carried out.

8. Discussion

Cyber space is a technology intensive field and has become a necessity in every spree of life as it makes systems efficient. Security of Information Systems has become a paramount important in the recent past. Another complexity in this field is that it is very dynamic and changes very quickly than the existing traditional system of regulatory and enforcement agencies.

Thus it's imperative that a practical and effective policy and security framework is put in place to avoid and legal implications which also affect the reputations of organizations.

9. Conclusion

The application and advantages of Information Systems in healthcare need no emphasis, however it's security aspects need special attention. It is pertinent that security aspects are included and considered right at the time of inception of any new system and thus all technical aspects of the security should be part of the design of any IT System. And of course, organizations need to keep themselves updated about the latest technology in order to utilize the best practices in the field of Cyber Security.

BIBLIOGRAPHY / REFERENCES

10.1 Ministry of Electronics and Information Technology, Government of India, White Paper of The Committee of Experts on A Data Protection Framework For India: http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (Accessed 25 April 2018).

10.2 Ministry of Health and Family Welfare, Government of India, Draft "Digital Information Security In Healthcare, Act (DISHA)": https://mohfw.gov.in/newshighlights/comments-draft-digital-information-security-health-care-actdisha (Accessed 15 April 2018).

10.3 Ministry of Electronics and Information Technology, Government of India, Information Technology Act 2000: http://meity.gov.in/content/information-technology-act-2000 (Accessed 10 May 2018).

10.4 Ministry of Electronics and Information Technology, Government of India, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011: http://meity.gov.in/sites/upload_files/dit/files/GSR313E _10511(1).pdf (Accessed 01 May 2018).

10.5 Ministry of Health and Family Welfare, Government of India, Electronic Health Record (EHR) Standards for India 2016: https://mohfw.gov.in/sites/default/files/17739294021483341357.pdf (Accessed 15 April 2018).

10.6 International Standard, ISO/IEC 27001, 2005: Information Technology – Security Technique- Information Management System-Requirements.

10.7 International Standard, ISO/IEC FDIS 17799, 2005: Information Technology – Security Technique- Code of Practice for Information Security Management.

10.8 Ministry of Electronics and Information Technology, Government of India, National Cyber Security Policy 2013: http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf (Accessed 20 April 2018).

10.9 United States Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA) of 1996: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (Accessed 15 April 2018).

Appendix A

SUMMARY OF: WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA

1. The Government of India has set up our Committee of Experts to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill. The objective of the paper is to "ensure growth of the digital economy while keeping personal data of citizens secure and protected."

2. **Committee**

Chairman: Justice B.N. Srikrishna

Members: Smt. Aruna Sundararajan
Dr. Ajay Bhushan Pandey
Dr. Ajay Kumar
Prof. Rajat Moona
Dr. Gulshan Rai
Prof. Rishikesha Krishnan
Dr. Arghya Sengupta
Smt. Rama Vedashree

3. The White Paper is very comprehensive consisting of 5 Parts covered in 243 pages. The committee has considered various aspects of framework for Data Protection and also compared existing framework of various developed countries. Provisional views of the committee are given in succeeding paragraphs.

4. **Key Principles of a Data Protection Law** A data protection framework in India must be based on the following seven principles:

(i) **Technology Agnosticism:** **"**The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance".

(ii) **Holistic Application:** **"**The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims".

(iii) **Informed consent:** **"**Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful".

(iv) **Data Minimisation:** **"**Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject".

(iv) **Controller Accountability**: " The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing"

.

(vi) **Structured Enforcement: "**Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms".

(vii) **Deterrent penalties**: "Penalties on wrongful processing must be adequate to ensure deterrence".

5. J**urisdiction: "**The power of the State to prescribe and enforce laws is governed by the rules of jurisdiction in international law. Data protection laws challenge this traditional conception since a single act of processing could very easily occur across jurisdictions. In this context, it is necessary to determine the applicability of the proposed data protection law".

6. Scope: "There are three issues of scope other than territorial application. These relate to the applicability of the law to data relating to juristic persons such as companies, differential application of the law to the private and the public sector, and retrospective application of the law".

7. Personal Data: "The definition of personal information or personal data is the critical element which determines the zone of informational privacy guaranteed by a data protection legislation. Thus, it is important to accurately define personal information or personal data which will trigger the application of the data protection law".

"Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while psuedonymised data continues to be personal data".

8. Sensitive Personal Data: "While personal data refers to all information related to a person's identity, there may be certain intimate matters in which there is a higher expectation of privacy. For instance, data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life".

9. Processing: "Data protection laws across jurisdictions have defined the term 'processing' in various ways. It is important to formulate an inclusive definition of processing to identify all operations, which may be performed on personal data, and consequently be subject to the data protection law".

10. Data Controller and Processor: "The obligations on entities in the data ecosystem must be clearly delineated".

11. Exemptions: **"**A data controller may be exempted from certain obligations of a data protection law based on the nature and purpose of the processing activity eg. certain legitimate aims of the state. The scope of such exemptions, also recognised by the Supreme Court in Puttaswamy needs to be carefully formulated".

12. Cross Border Flow of Data: **"**Given the advent of the Internet, huge quantities of personal data are regularly transferred across national borders. Providing strong rules to govern such data flows is vital for all entities in the data eco-system".

13. Data Localisation: **"**Data localisation requires companies to store and process data on servers physically located within national borders. Several governments, driven by concerns over privacy, security, surveillance and law enforcement, have been enacting legislations that necessitate localisation of data. Localisation measures pose detrimental effects for companies may, harm Internet users, and fragment the global Internet".

14. Allied Laws: **"**Currently, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. These laws operate in various sectors, such as, the financial sector, health sector and the information technology sector. Consequently, such laws may need to be examined against a new data protection legal and regulatory framework as and when such framework comes into existence in India".

Grounds of Processing, Obligation on Entities and Individual

15. Consent: **"**Most jurisdictions treat consent as one of the grounds for processing of personal data. However, consent is often not meaningful or informed, which raises issues of the extent to which it genuinely expresses the autonomous choice of an individual. Thus, the validity of consent and its effectiveness needs to be closely examined".

16. Child's Consent: **"**It is estimated that globally, one in three Internet users is a child under the age of 18. Keeping in mind their vulnerability and increased exposure to risks online, a data protection law must sufficiently protect their interests".

17. Notice: **"**Notice is an essential prerequisite to operationalise consent. However, concerns have been raised about notices being ineffective because of factors such as length, use of complex language, etc. Thus, the law needs to ensure that notices are effective, such that consent is meaningful".

18. Grounds of Processing: **"**It is widely recognised that consent may not be sufficient as the only ground for lawful processing of personal data. Several other grounds, broadly conforming to practical requirements and legitimate state aims, are incorporated in various jurisdictions. The nature and remit of such grounds requires determination in the Indian context".

19. Purpose Specification and Use Limitation: **"**Purpose specification and use limitation are two cardinal principles in the OECD framework. The principles have two components- first, personal data must be collected for a specified purpose; second, once data is collected, it must not be processed further for a purpose that is not specified at the time of collection or in a manner incompatible with the purpose of collection. However the relevance of these principles in the world of modern technology has come under scrutiny, especially as future uses of personal data after collection cannot always be clearly ascertained. Its relevance for the Indian context will thus have to be assessed".

20. Processing of Sensitive Personal Data: "If 'sensitive personal data' is to be treated as a separate category, there is a concomitant need to identify grounds for its processing. These grounds will have to be narrower than grounds for general processing of personal data and reflect the higher expectations of privacy that individuals may have regarding intimate facets of their person".

21. Storage Limitation and Data Quality: **"**Related to the principle of purpose specification is the principle of storage limitation which requires personal data to be erased or anonymised once the purpose for which such data was collected is complete. Personal data in the possession of data controllers should also be accurate, complete and kept up-to-date. These principles cast certain obligations on data controllers. The extent of such obligations must be carefully determined".

22. Individual Participation Rights: **"**One of the core principles of data privacy law is the "individual participation principle" which stipulates rights of confirmation, access, and rectification. Incorporation of such rights has to be balanced against technical, financial and operational challenges in implementation".

23. Individual Rights to Processing: **"**In addition to confirmation, access and rectification, individual should have right to object to processing (including for Direct marketing), the right not to be subject to a decision solely based on automated processing, the right to restrict processing, and the right to data portability".

24. Individual Rights "to be forgotten" : **"**The right to be forgotten has emerged as one of the most emotive issues in data protection law".

25. <u>Enforcement Models: Regulation and Enforcement</u>

(i) Command and Control.
(ii) Self-regulation.
(iii) C-regulation (preferred model).

26. Accountability: **"**A responsible Data Controller must ensure that it secures the integrity and confidentiality of personal information in its possession by taking appropriate technical and organisational measures in order to prevent loss, damage, or

unauthorised destruction of personal information. Data Controllers should be liable for any harm caused to individuals".

27. <u>Enforcement Tools</u>

.

(a) Codes of Practice

(b) Personal Data Breach Notification

(c) <u>Categorisation of Data Controllers</u>

(i) Registration.
(ii) Data Protection Impact Assessment (DPIA).
(iii) Data Protection Audit.
(iv) Data Protection Officer.
(v) Data Protection Authority

27. Data Protection Authority: "A separate and independent data protection authority may be set up in India for enforcement of a data protection legal framework".

27. Adjudication Process: "Data Protection Authority should adjudicate on disputes arising between an individual and a data controller due to breach of any data protection obligation".

28. <u>Remedies</u>

(a) <u>Penalties</u> Possible calculations for civil penalties are as follows:

(i) Per day basis;
(ii) Discretion of the adjudicating body subject to a fixed upper limit;
(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter (such as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller).

(b) Compensation: "An individual may be given the right to seek compensation from a data controller in case the person has suffered any loss or damage due to a violation of the data controller's obligations under a data protection legal framework".

(c) Offences: "The law may treat certain actions of a data controller as an offence and impose a criminal liability. This may include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject".

Appendix B

DRAFT CYBER SECURITY POLICY FOR HEALTHCARE

1. INTRODUCTION

1.1 Information Systems have become a necessity in every sphere of life and healthcare is no exception. These Systems have complex design owing to their multiple interactions between people, software, data (which may at multiple locations) along with utilisation of various Information Communication Technology (ICT) devices and networks.

1.2 Due to the numerous applications & benefits of Information Systems brought about by rapid technological advancements, these systems are utilised by citizens, businesses, healthcare providers, military and governments. These Systems are expected to become more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

1.3 Information Technology (IT) has emerged as one of the most significant growth catalysts for the Indian economy. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways).

1.4 Information Technology is expected to play very important role in provision of effective and efficient healthcare services to all citizens at affordable cost in the near future. Accordingly, government has ambitious plans for creation of infrastructure for Health IT. This has necessitated focus on Cyber Security issues with the aim of creating a secure computing environment with adequate trust & confidence in electronic transactions, software, services, devices and networks. Such a focus enables creation of a suitable cyber security eco-system, in tune with globally networked environment.

1.5 Cyber Security Policy is an evolving task and it caters to the whole spectrum of ICT users. It provides a framework for defining and guiding the actions related to security of IT Systems. The policy provides an overview of actions required to effectively protect information systems & networks. This policy, therefore, aims to create a cyber security framework to enhance the security of Health Information Technology Systems.

2. Vision, Mission & Objectives

2.1 Vision

To build a secure and resilient healthcare cyberspace for citizens, businesses and Government**.**

2.2 Mission

To protect IT Systems related to healthcare, reduce vulnerabilities & damage from cyber incidents and respond to cyber threats through a combination of institutional structures, people, processes, technology and cooperation.

2.3 Objectives

2.3.1. To create a secure healthcare cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of Health IT in all government and private sectors.

2.3.2 To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

2.3.3 To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

2.3.4. To enhance and create Health Cyber Security Cell for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

2.3.5. To encourage healthcare facilities to adopt standard security practices and processes.

2.3.6. To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

3. RISK ASSESSMENT AND TREATMENT

The first step before formulation of cyber security policy for an organisation is to carry out Risk Assessment, Risk Acceptance along with objectives of the organisation.

3.1. Assessing security risks

All healthcare facilities and organisations should carry out risk assessment and identify, quantify, and prioritize risks against criteria for risk acceptance and considering overall objectives of the organization. The outcome of the assessment should guide the appropriate management actions including controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be repeated for formulation of an effective cyber security policy.

3.2. Risk Assessment in Healthcare within an Orgnisation

3.2.1. Unauthorised access at Healthcare facility / organisation by an insider.
3.2.2. Unauthorised possession / stealing of IT system, like computer, laptop.
3.2.3 Unauthorised interception of data during transfer from one organisation to another.
3.2.3 Hacking.
3.2.4 Virus and Trojan Horse.
3.2.5 Malicious code in a software .

3.3 Treating security risks

For each of the risks identified during the risk assessment, a risk treatment decision needs to be made. Possible options for risk treatment include:
a) Applying appropriate controls to reduce the risks.
b) Avoiding risks by not allowing actions that would cause the risks to occur by putting proper procedures in place.

4.0 Strategies

4.1 Creating a secure cyber ecosystem

4.1.1 Ministry of Health and Family Welfare (MoHFW) plans to set up National Digital Health Authority (NDHA) through an Act of Parliament. The proposed NDHA will also be responsible as National Nodal Agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

4.1.2 To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

4.1.3 To encourage all organizations to develop information security policies duly integrated with their business plans.

4.1.4 To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

4.1.5 To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

4.1.6 To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

4.1.7 To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

4.1.8 To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

4.2 Creating an assurance framework

4.2.1 To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

4.2.2 To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

4.2.3 To encourage secure application / software development processes based on global best practices.

4.2.4 To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

4.3 Strengthening the Regulatory framework

4.3.1 To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance. NDHA will carry out task of regulatory body.

4.3.2 To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

4.3.3 To enable, educate and facilitate awareness of the regulatory framework.

4.4. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

4.4.1 To operate a 24x7 National Level Computer Emergency Response Team - Health(CERT-H) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management.

4.4.2. To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

4.5. Securing Services

4.5.1. To enforce and educate healthcare providers the use of standard secure / encrypted protocol, like HL7 for data exchange.

4.5.2. To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

4.6. Promotion of Research & Development in Cyber Security

4.6.1 NDHA shall encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

4.6.2 To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

4.7 Reducing supply chain risks

4.7.1 NDHA shall create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

4.7.2 NDHA shall create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

4.8 Human Resource Development

4.8.1 To foster education and training programs both in formal and informal sectors to support Health cyber security needs and build capacity.

4.8.2 To manage password when new employee is inducted and when the employee leaves the organization.

4.9 Creating Cyber Security Awareness

4.9.1 To promote and launch a comprehensive national awareness program on security of Health cyberspace.

4.9.2 To conduct, support and enable cyber security workshops / seminars and certifications.

Appendix C

COMMENTS FORWARDED TO MoHFW ON DRAFT "DIGITAL INFORMATION SECURITY IN HEALTHCARE (DISHA) ACT"

1. **Nomenclature: NDHA vs NeHA** As per the MoHFW covering letter dt 21 Mar 2018 regarding comments on the draft Act, National Digital Health Authority (NDHA) is proposed to be set up, however, as per Section 4, Chapter II of the proposed Act National Electronic Health Authority (NeHA) shall be established.

Recommendation Any one nomenclature be taken. NeHA is broader term thus recommended.

2. **Para 3(1)(c): Consent**

As per IT Act 2000, any electronic document which is not digitally signed is equivalent to unsigned paper document. However, Consent (in physical or paper form) has to be signed by an individual, thus Consent taken in electronic form should be digitally signed.

Recommendation: Paragraph may be amended as below:

'Consent' means expressed informed consent, whether in written or electronic form (duly digitally signed), given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data.

3. **Para 3(1)(e): 'Digital Health Data'**

Following may be added:
(i) EMR/EHR.
(ii) Lab reports.
(iii) Radiographic reports.
(iv) Medicines consumed while admitted in a hospital/ prescribed by a doctor.
(v) Payment made to the healthcare provider by an individual directly or through Health Insurance Company.

4. **Para 3(1)(k): 'Personally Identifiable Information'**

It is recommended that instead of 'Personally Identifiable Information', 'Protected Health Information' may be used, as it is more relevant in the present case. And following details may be included for 'Personally Identifiable Information' or 'Protected Health Information' in Schedule I :

(I) Name.
(II) Geographical identifiers smaller than a state i. e. District and below.

(III) Dates (other than year) directly related to an individual.
(IV) Phone/ FAX Numbers.
(V) Email addresses.
(VI) Medical record numbers.
(VII) Health insurance beneficiary numbers.
(VIII) Bank Account numbers/Debit/Credit Card details.
(IX) License numbers.
(X) Vehicle identifiers i.e. RC numbers.
(XI) Web Uniform Resource Locators (URLs) and Internet Protocol (IP) address numbers.
(XII) Biometric identifiers, including finger, retinal and voice prints.
(XIII) Full face photographic images and any comparable images.
(XIV) Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL').

(XV) Any other unique identifying number.

5. **Para 3(1)(n): 'Data Security'** Data related to Protected Health Information (PHI) needs to be secured and not only the Digital Health Data which is subset of the PHI.

Recommendation Paragraph may be amended as below

'Data Security' refers directly to "Protected Health Information (PHI)", and specifically to the means used to protect the privacy of health information contained in digital health data that supports professionals in holding that information in confidence.

6. **Para 3(1)(o): 'Sensitive Health Related Information"**

This is little confusing as a term 'Digital Health Data' has also been mentioned at Section 3(1)(c). All data related to health should be considered as sensitive, however this paragraph is giving an impression as if only some data related health is sensitive and not the complete health data .

Recommendation Paragraph 3(1)(o) should be deleted.

7. **Section 28(1): The rights of the owner of digital health data**

The owner of the heath data has the right to privacy and a Clinical Establishment has to implement it by ensuring security of this data.

Recommendation The paragraph may be amended as under:

An owner shall have the right to privacy of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.

8. **Section 28(2): The rights of the owner of digital health data**

This section contradicts the provisions of Section 29 to quite an extent. Electronic Health data is an equivalent of physical records being maintained by clinical establishments and these are very much required so no consent seems to be essential for maintaining legitimate medical records. In fact it is mandatory to maintain medico legal cases. Thus this section should be amended as Clinical Establishment needs to collect and store health data for provision of requisite healthcare services and for future use for benefit of an individual also, so an individual should be given right to give consent to share his/her information along with individually identifiable information or not, like for research.

9. **Section 28(3) and Section 28(4): The rights of the owner of digital health data**

An individual's right should be limited to give consent to share his/her information along with individually identifiable information or not.

10. **Section 41, 42: Obtaining Digital Health Information of another Person & Data Theft**

Similar such crimes i.e. data theft and fraudulently obtaining data, are covered under IT Act 2000, so provisions of IT Act 2000 should be made applicable otherwise there can be confusion if punishments are not same in both the Acts.