

From

To

The Secretary Health,
Chandigarh Administration.

1. The Director Principal,
Govt. Medical College and Hospital,
Sector-32, Chandigarh.
2. The Director Health & Family Welfare,
U.T. Chandigarh

No.917/F-II(GMSH)/2018/ 5805
Dated, Chandigarh the 13/4/18

Subject:- Regarding Digital information Security in Healthcare (DISHA).

Enclosed please find herewith a copy of D.O. No. Z-18015/23/2017-eGov dated 22-3-2018 alongwith its enclosures received from Joint Secretary, Govt. of India, Ministry of Health & Family Welfare, Nirman Bhawan, New Delhi on the subject cited above for taking necessary action in the matter.

DA: As above

For Superintendent Health,
Secretary Health,
Chandigarh Administration.

GOVERNMENT MEDICAL COLLEGE & HOSPITAL SECTOR-32, CHANDIGARH
HOSPITAL ADMINISTRATION BRANCH-II

Endst.No.GMCH-HA-II-EA3 (15)/2018/ 9201/

Dated:-

A copy is forwarded to the System Analyst, IT Centre, GMCH with a request to e-circulate/email the same to All the HODs, GMCH-32, Chandigarh with the request to send their opinion within 7-days to proceed further in the matter

for - Office Superintendent (HA-II)
Joint Medical Superintendent



PA/AS- 3355

Dated 5/4/18



सत्यमेव जयते

भारत सरकार
स्वास्थ्य एवं परिवार कल्याण मंत्रालय
निर्माण भवन, नई दिल्ली - 110011

Government of India
Ministry of Health & Family Welfare
Nirman Bhavan, New Delhi - 110011

D.O. No. Z-18015/23/2017-eGov

Dated: 22nd March, 2018

AV AGARWAL, IAS

Joint Secretary

Tel: 011-23061195

T/Fax: 011-23061842

E-mail: alav@ias.nic.in

Dear Sir,

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a 'sensitive data' which deserves to be protected more than other forms of 'personal data'. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders.

Salient features of draft Act include:

- Expressing the 'ownership' of 'digital health data' (with the person/patient to whom the digital health data belongs to)
- Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- Providing for establishment of Digital Health Information Exchanges; and
- Framework to provide for civil and criminal remedies for data breach.

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act for seeking your comments and suggestion on the draft act before putting this up in public domain for feedback.

With Regards,

Yours sincerely,

[Lav Agarwal]

Shri Anurag Agarwal
Home Secretary-cum-Secretary
(Health & Family Welfare),
UT Secretariat, Deluxe Building,
Sector-9, Chandigarh- 160017

Rec Above

Rec Bearing D.O. No.
Health-917, D.O.
06/4/18 (pages 1 to 33)
has been placed below.
Rw (GMSU) to endow-61

09/4/18

Health Branch
Diary No: 917
Dated: 06/4/18

**Digital Information Security in Healthcare,
Act**

[Draft for Public Consultation]

November, 2017

**Ministry of Health & Family Welfare,
Government of India**

INDEX

| SL. NO. | PARTICULARS | PAGE NO. |
|---------|--|----------|
| 1 | CHAPTER I – PRELIMINARY | 2 |
| 2 | CHAPTER II - NATIONAL ELECTRONIC HEALTH AUTHORITY | 6 |
| | STATE ELECTRONIC HEALTH AUTHORITIES | |
| | HEALTH INFORMATION EXCHANGES | |
| 3 | CHAPTER III – POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES | 13 |
| 4 | CHAPTER IV - DATA OWNERSHIP, SECURITY AND STANDARDIZATION | |
| 5 | CHAPTER V- DIGITAL HEALTH DATA BREACH AND CONSEQUENCES | 24 |
| 6 | CHAPTER VI- ADJUDICATING AUTHORITY | 27 |
| 7 | CHAPTER VII- MISCELLANEOUS PROVISIONS | 31 |

Digital Information Security in Healthcare Act (INSERT YEAR)

An Act to provide for establishment of National and State eHealth Authorities and Health Information Exchanges; to standardize and regulate the processes related to collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security of digital health data and such other matters related and incidental thereto.

BE IT ENACTED by Parliament in (insert year) of the Republic of India as follows:

CHAPTER I PRELIMINARY

1. SHORT TITLE, EXTENT

- (1) This Act may be called as Digital Information Security in Healthcare Act (DISHA) (insert year).
- (2) It extends to whole of India except the State of Jammu and Kashmir.

2. COMMENCEMENT AND APPLICATION

- (1) This Act shall come into force on such date as the Central Government may, by notification, appoint; and different dates may be appointed for different States and for different provisions of this Act.

3. DEFINITIONS

- (1) In this Act, unless the context otherwise requires,
 - (a) **'Anonymization'** means the process of permanently deleting all personally identifiable information from an individual's digital health data.
 - (b) **'Breach'** shall have the same meaning as assigned to it in Section 37 of this Act.
 - (c) **'Consent'** means expressed informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data.

Provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act.

- (d) **'De-identification'** means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's digital health data in a manner that

eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.

- (e) **'Digital Health Data'** means an electronic record of health-related information about an individual and shall include the following:
- (i) Information concerning the physical or mental health of the individual;
 - (ii) Information concerning any health service provided to the individual;
 - (iii) Information concerning the donation by the individual of any body part or any bodily substance;
 - (iv) Information derived from the testing or examination of a body part or bodily substance of the individual;
 - (v) Information that is collected in the course of providing health services to the individual; or
 - (vi) Information relating to details of the clinical establishment accessed by the individual.
- (f) **'Entity'** includes any of the following, not being a clinical establishment:
- (i) An individual;
 - (ii) A company;
 - (iii) A department of the Central or State Government;
 - (iv) A firm;
 - (v) An association of persons or a body of individuals, whether incorporated or not, in India or outside India; or
 - (vi) Any corporation established by or under any Central, State or Provincial Act or a Government company as defined in section 2(45) of the Companies Act, 2013;
 - (vii) Any body corporate incorporated by or under the laws of a country outside India;
 - (viii) A co-operative society registered under any law relating to cooperative societies;
 - (ix) A local authority;
 - (x) Every artificial juridical person, not falling within any of the preceding sub-clauses;
- (g) **'Guardian'** means a guardian recognised under any law for the time being in force.
- (h) **'Health Information Exchange'** means a health information exchange as established under this Act.

- (i) **'Clinical Establishment'** means (i) a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognised system of medicines established and administered or maintained by any person or body of persons, whether incorporated or not; or (ii) a place established as an independent entity or part of an establishment referred to in sub-clause (i), in connection with the diagnosis where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not, and shall include a clinical establishment owner, controlled or managed by
- a. the Government or a department of the Government;
 - b. a trust, whether public or private;
 - c. a corporation (including a society) registered under a Central, Provincial or State Act, whether or not owned by the Government;
 - d. a local authority;
 - e. a single doctor,
- but does that include the clinical establishments owned, controlled or managed by the Armed Forces.
Explanation: For the purpose of this clause, "Armed Forces" means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)
- (j) **'Owner'** means an individual whose digital health data is generated and processed under this Act.
- (k) **'Personally Identifiable Information'** means any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person, and includes the information stated in Schedule I.
- (l) **'Prescribed'** shall mean rules prescribed by the Central Government or the State Governments as the case may be.
- (m) **'Relative'** with reference to the owner, means—
- (i) spouse of the owner;
 - (ii) parents of the owner;
 - (iii) brother or sister of the owner;

- (iv) brother or sister of the spouse of the owner;
 - (v) brother or sister of either of the parents of the owner;
 - (vi) in the absence of any of the relatives mentioned at sub-clauses (i) to (v), any lineal ascendant or descendant of the owner;
 - (vii) in the absence of any of the relatives mentioned at sub-clauses (i) to (vi), any lineal ascendant or descendant of the spouse of the owner;
- (n) **'Data Security'** refers directly to protection of digital health data, 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.
- (o) **'Sensitive health-related information'** means information, that if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, violence, discrimination or unfairness to an individual, including but not limited to, one's physical or mental health condition, sexual orientation, use of narcotic or psychotropic substances, consumption of alcohol, sexual practices, Human Immunodeficiency Virus status, Sexually Transmitted Infections treatment, and abortion.
- (p) **'serious breach'** shall have the same meaning as assigned to it in Section 38 of this Act.
- (q) **'Specified'** shall mean as specified by National eHealth Authority of India or State eHealth Authority, as the case may be.
- (r) **"need to know basis"** means the access to digital health data by a specific person for a specific and lawful purpose that is necessary for that purpose or to carry out that function.

CHAPTER II

NATIONAL ELECTRONIC HEALTH AUTHORITY OF INDIA, STATE ELECTRONIC HEALTH AUTHORITIES AND HEALTH INFORMATION EXCHANGES

4. National Electronic Health Authority of India (NeHA)

- (1) The Central Government shall establish for the purposes of this Act, a National Electronic Health Authority of India, by Notification in the

Official Gazette, which may be referred to as NeHA in its abbreviated form.

- (2) The National Electronic Health Authority of India, shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the Central Government, specifies a separate date in the same Notification.

5. Composition of National Electronic Health Authority of India

- (1) National Electronic Health Authority of India shall consist of the following members, to be appointed by the Central Government by Notification, namely:
- (a) A full time Chairperson;
 - (b) A member -secretary; equivalent to the rank of Joint Secretary to the Government of India
 - (c) Four full-time members to be appointed by the Central Government:
 - (i) One from health informatics;
 - (ii) One from public health;
 - (iii) One from law; and
 - (iv) One from public policy
 - (d) Four ex-officio members, not less than the rank of Joint Secretary to the Government of India to be appointed by the Central Government:
 - (i) One from Ministry of Electronics and Information Technology;
 - (ii) One from Ministry of Panchayati Raj/ Ministry of Women & Child Development;
 - (iii) One from Directorate General of Health Services; and
 - (iv) One from Ministry of Law and Justice
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
- (a) Be not more than sixty-five years of age;
 - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Fifteen years in any of the following areas or a combination thereof:
 - (i) Information Technology (IT);
 - (ii) Health Informatics; or
 - (iii) Public Health; or
 - (iv) Law; or
 - (v) Public policy.
- Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building.
- (3) The National Authority shall be a body corporate with the name specified by the Central Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and

dispose of property and to contract, and may, by the said name, sue or be sued.

6. National Executive Committee

- (1) The Central Government shall, immediately after the notification under sub-section (1) of Section 4, constitute a National Executive Committee to assist the National Authority in the performance of its functions under this Act.
- (2) The National Executive Committee shall consist of the following members, namely:-
 - (a) Additional Secretary/Joint Secretary, ehealth as Chairperson;
 - (b) Deputy Commissioner/Assistant Commissioners as members;
 - (c) Director/Deputy Secretary as member; and
 - (d) Supported by consultants and ehealth section.
- (3) The Chairperson of the National Executive Committee may invite any other officer of the Central Government or a State Government for taking part in any meeting of the National Executive Committee and shall exercise such powers and perform such functions as may be prescribed by the Central Government in consultation with the National Authority.
- (4) The procedure to be followed by the National Executive Committee in exercise of its powers and discharge of its functions shall be such as may be prescribed by the Central Government.

7. State Electronic Health Authorities

- (1) Every State Government shall, as soon as may be after the issue of the notification under sub-section (1) of section 4, by notification in the Official Gazette, establish a State Electronic Health Authority, which may be referred to as SeHA in its abbreviated form.
- (2) The State Electronic Health Authority shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the State Government, specifies a separate date in the same Notification.

8. Composition of State Electronic Health Authorities

- (1) State Electronic Health Authority shall consist of the following members, to be appointed by the State Government by Notification, namely:
 - (a) A full time Chairperson;
 - (b) Secretary in-charge of State Health Department or equivalent as member-secretary;
 - (c) Three full-time members to be appointed by the State Government:
 - (i) One from health informatics;
 - (ii) One from public health; and
 - (iii) One from law

- (d) Three ex-officio members to be appointed by the State Government:
 - (i) Director, State Health Services;
 - (ii) One from State Information Technology department; and
 - (iii) One from State Law department
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
 - (a) Be not more than sixty-five years of age;
 - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Twelve years in any of the following areas or a combination thereof:
 - (i) Information Technology (IT);
 - (ii) Health Informatics; or
 - (iii) Public Health; or
 - (iv) Law; or
 - (v) Public policy.

Provided that; to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building.
- (3) The State Authority shall be a body corporate with the name specified by the State Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and dispose of property and to contract, and may, by the said name, sue or be sued.

9. State Executive Committee

- (1) The State Government shall, immediately after issue of notification under sub-section (1) of section (7), constitute State Executive Committee to assist the State Authority in the performance of its functions, under this Act.
- (2) The State Executive Committee shall consist of the following members, namely:—
 - (a) The Secretary Health, as the Chairperson;
 - (b) Director, Health Services as member;
 - (c) Deputy Secretary ehealth as member; and
 - (d) Supported by consultants and ehealth section.
- (3) The Chairperson of the State Executive Committee shall exercise such powers and perform such functions as may be prescribed by the State Government and such other powers and functions as may be delegated to him by the State Authority.
- (4) The procedure to be followed by the State Executive Committee in exercise of its powers and discharge of its functions shall be such as may be prescribed by the State Government.

10. Term of Office of Chairperson & other members of National and State Authorities

- (1) The Chairperson and members of the National Authority, shall hold office for a term of three years, as the Central Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (2) The chairperson and members of the State Authority, shall hold office for a term of three years, as the State Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (3) The Chairperson and other Members, appointed as per sub-section (1) of section 5 and sub-section (1) of section 8, are eligible for reappointment for another term; provided such reappointed Chairperson or Member does not exceed sixty-five years of age.

11. Salary, allowance, benefits and service conditions etc.,

- (1) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members of the National Authority, shall be such as may be prescribed by the Central Government.
- (2) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members of the State Authorities, shall be such as may be prescribed by the State Governments.
- (3) Notwithstanding anything stated in sub-section (1) and (2) above, the salary, allowances and other conditions of service of the Chairperson or of a member shall not be varied to his disadvantage after his appointment.

12. Reconstitution of the National and State Authorities

- (1) Any vacancy caused to the office of the Chairperson or any other member of the National & State Authority shall be filled up by the Central Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (2) Any vacancy caused to the office of the Chairperson or any other member of the State Authority shall be filled up by the State Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (3) In the event of vacancy in the office of the Chairperson of the National or State Authority, the senior most person, from amongst the full time members, shall act as the Chairperson, till the vacancy is filled.
- (4) No act or proceeding of the National or State Authority shall be invalid merely by reason of-
 - (a) Any vacancy in, or any defect in the constitution of the Authority; or
 - (b) Any defect in the appointment of a person acting as a member of the Authority; or

- (c) Any irregularity in the procedure of the Authority not affecting the merits of the case.

13. Temporary association of persons with National or State Authorities for particular purposes –

- (1) The National Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (2) A State Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (3) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall have a right to take part in the discussions of the Authority relevant to that purpose, but shall not have a right to vote at a meeting of the Authority, and shall not be a member for any other purpose.
- (4) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall be paid such fees and allowances, for attending its meetings and for attending to any other work of the Authority, as may be prescribed.

14. Officers and Other Employees of the National and State Authorities

- (1) The National Authority, in consultation with Central Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (2) The State Authority, in consultation with the State Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (3) The salary and allowances payable to; and the other conditions of service of the officers and other employees of the National or State Authority appointed under sub-section (1) and (2) shall be such as may be prescribed.

15. Meetings

- (1) The National Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be prescribed by Central Government by Rules under this Act.
- (2) The State Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be prescribed by Central Government by Rules under this Act.
- (3) The chairperson of the National or State Authority, if unable to attend a meeting, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.

16. Disqualifications

- (1) A person shall be disqualified for appointment as Chairperson or member of the National Electronic Health Authority or a State Electronic Health Authority, if he/she –
 - (i) Has been convicted and sentenced to imprisonment for an offence which, in the opinion of the Central Government, involves moral turpitude; or
 - (ii) Is an undercharged insolvent; or
 - (iii) Has been removed or dismissed from the service of the Government or a body corporate owned or controlled by the Government; or
 - (iv) Has in the opinion of the Central Government, such financial or other interest as is likely to affect prejudicially the discharge by him of his functions as a member; or
 - (v) Has such other disqualification as may be prescribed by the Central Government.

17. Resignation, removal of chairperson or member of the National or State Authorities

- (1) The Chairperson or full time member of the National Authority appointed under sub-section (1) of section 5 and the Chairperson or full time member of a State Authority appointed under sub-section (1) of section 8:
 - (a) May relinquish his/her office by submitting the resignation in writing to the Central Government or the State Government as the case may be; or
 - (b) May be removed from his/her office in accordance with the provisions of section 18.

18. Removal in certain circumstances

- (1) The Central Government or the State Government, may remove from office the Chairperson or any full-time member of the National or State Authority, who –
 - (a) Has been adjudged as an insolvent; or
 - (b) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
 - (c) Has become physically or mentally incapable of discharging his or her functions; or
 - (d) Has acquired such financial or other interest as is likely to affect prejudicially his or her functions as the Chairman or member; or
 - (e) Has so abused his/her position as to render his or her continuance in office prejudicial to the public interest.
- (2) No such member or Chairperson shall be removed from his/her office under clause (d) or clause (e) of sub-section (1) above, unless he/she has been given a reasonable opportunity of being heard in the matter.

19. Health Information Exchanges

- (1) The Central Government shall, by notification, establish as many Health Information Exchanges, as considered necessary, for the purposes for this Act
- (2) No entity shall function as a Health Information Exchange unless established as such by the central Government

20. Management of Health Information Exchange

- (1) All Health Information Exchanges shall conduct and carry out their affairs strictly as per the norms, standards or protocols specified by the National Electronic Health Authority, from time to time, or as per the Rules prescribed by the Central Government.
- (2) Without prejudice to any other stipulations of this Act, a Health Information Exchange established under section 19 shall only employ such skilled personnel for management of its affairs as may be specified by the National Electronic Health Authority.
- (3) Conditions with respect to periodical reports, annual reports and direct inquiries may be such as may be prescribed by the Central Government.

21. The Chief Health Information Executive and his functions

- (1) The Health Information Exchange shall have a Chief Health Information Executive, abbreviatedly referred to as CHIE, who shall possess such qualifications and experiences as may be prescribed by the Central Government as rules under this Act;
- (2) The Chief Health Information Executive as appointed under sub-section (1) above, shall be the Chief Executive Officer and also the data controlling authority of the Health Information Exchange, and be responsible for all routine and day-to-day affairs, and in particular:
 - (a) Ensure the day-to-day affairs of the Health Information Exchange runs smoothly and as per the objectives and norms of this Act.
 - (b) Access, and process the digital health care data transmitted by the Clinical Establishments to further transmit the digital health care data, whenever required, in accordance with norms prescribed by the National Electronic Health Authority of India.
 - (c) Take appropriate measures to maintain, secure and protect the digital health care data as prescribed by the National Digital Health Authority of India.
 - (d) Notify the data breach to the owner and such other concerned.
 - (e) Store the digital health care data in prescribed mode in all situations.

CHAPTER III

POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES

22. Powers and functions of National Electronic Health Authority of India

- (1) The National Electronic Health Authority of India in order to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
 - (a) Formulate standards, operational guidelines and protocols for the generation, collection, storage and transmission of the digital health data for the purposes of this Act, applicable to:
 - (i) Clinical establishments generating and collecting digital health data for their own use or for further transmission to the health information exchanges;
 - (ii) Health information exchanges storing and transmitting digital health data to clinical establishments, or to other health information exchanges, or to State Electronic Health Authority, or the National Electronic Health Authority;
 - (iii) Any other entity having custody of any digital health data;
 - (iv) State Electronic health Authority and the National Electronic Health Authority;
 - (b) To ensure data protection and prevent breach or theft of digital health data, establish data security measures for all stages of generation, collection, storage and transmission of digital health data, which shall at the minimum include access controls, encrypting and audit trails;
 - (c) Conduct periodical investigations to ensure compliance with the provisions of this Act and any rules, regulations, standards or protocols hereunder by health information exchanges;
 - (d) Notify and mandate the health information exchanges, in case of failure to comply with the provisions of this Act;
 - (e) To lay down protocol for transmission of digital health data to and receiving it from other countries;
 - (f) Collaborate and work with Standardization Testing and Quality Certification of digital health care system, by establishing necessary norms and institutions, including collaborating with existing institutions;
 - (g) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (g) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed

23. National Authority's power of oversight, inspection, investigation and issuance of directions etc.

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the National Electronic Health Authority or its representative, shall have the right to inspect all such records; or access the premises, including virtual premises of the health information exchange or exchanges at any time.

Provided that National Electronic Health Authority, while accessing such records or accessing either the physical or virtual premises of health information exchanges, shall bear in mind that no or least possible hindrance is caused to the normal working of the health information exchange.

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the National Electronic Health Authority to generally discharge its functions under this Act, shall direct a health information exchange or class of health information exchanges, or all health information exchanges as the case may be, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the National Electronic Health Authority, shall be binding upon the health information exchange or health information exchanges.

24. Powers and Functions of State Electronic Health Authorities

- (1) The State Electronic Health Authority to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
 - (a) Ensure that the clinical establishments and other entities in the state collect, store, transmit and use digital health data as per the provisions of this Act and the standards, protocols and operational guidelines issued by the National Electronic Health Authority, from time to time;
 - (b) Conduct investigations to ensure compliance with the provisions of this Act;
 - (c) Notify and mandate the clinical establishments and other entities, in case of failure to comply with the provisions of this Act;
 - (d) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (c) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed by the Central Government.

25. State Authority's power of Oversight, inspection, investigation and issuance of directions etc.

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the State Electronic Health Authority, or its representative, shall have the right to inspect all such records; or access the premises including virtual premises, of a Clinical establishment or other entities at any time.

Provided that State Electronic Health Authority while accessing such records or accessing the physical premises of Clinical establishments, shall bear in mind that no or least possible hindrance is caused to the normal working of the clinical establishment

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the State Electronic Health Authority to generally discharge its functions under this Act, it shall direct a clinical establishment or a class of clinical establishments, or all clinical establishments as the case may be, or entities, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the State Digital Health Authority are binding upon the clinical establishment or clinical establishments and entities as the case may be.

26. Power of Civil Court – Notwithstanding anything contained in any other law for the time being in force, the National Authority while exercising the powers under section 23 and the State Authorities while exercising the powers under section 25, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:-

- (a) summoning and enforcing the attendance of witnesses and examining them on oath;
- (b) discovery and production of any document;
- (c) receiving evidence on affidavit;
- (d) requisitioning any public record or copy thereof from any court or office;
- (e) issuing commissions for examination of witnesses or documents;
- (f) any other matter which may be prescribed

27. Power to give directions –

- (1) In the performance of its functions under this Act, -
 - (a) The National Authority shall be bound by such directions in writing as the Central Government may give to it;
 - (b) Every State Authority shall be bound by such direction in writing as the National Authority or the State Government may give to it;

Provided that where a direction given by the State Government is inconsistent with the direction given by the National Authority, the matter shall be referred to the Central Government for its decision, which shall be final.

- (c) Every Health Information Exchange shall be bound by such directions in writing as the National Authority may give to it;
- (d) Every Clinical Establishment shall be bound by such directions in writing as the State Authority may give to it.

CHAPTER IV

DATA OWNERSHIP, SECURITY AND STANDARDIZATION

28. The rights of the owner of digital health data

- (1) An owner shall have the right to privacy, confidentiality, and security of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.
- (2) An owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, subject to the exceptions provided in Section 29 of this Act.
- (3) An owner shall have the right to give, refuse or withdraw consent for the storage and transmission of digital health data.
- (4) An owner shall have the right to refuse consent to the access or disclosure of his or her digital health data, and if refused it shall not be disclosed, subject to the exceptions provided in Section 33 of the Act.
- (5) An owner of the digital health data shall have the right that the digital health data collected must be specific, relevant and not excessive in relation to the purpose or purposes for which it is sought;
- (6) An owner of the digital health data shall have the right to know the clinical establishments or entities which may have or has access to the digital health data, and the recipients to whom the data is transmitted or disclosed;
- (7) The owner of the digital health data shall have a right to access their digital health data with details of consent given and data accessed by any Clinical Establishment/Entity;
- (8) The owner of the digital health data shall have, subject to sub-section (1) to (3) above:
 - (a) The right to rectify without delay, from the respective clinical establishment or health information exchange or entity, any inaccurate or incomplete digital health data, in the prescribed form as may be notified by the National Electronic Health Authority;
 - (b) The right to require their explicit prior permission for each instance of transmission or use of their digital health data in

- an identifiable form, through such means as may be prescribed by the Central Government;
- (c) The right to be notified every time their digital health data is accessed by any clinical establishment within the meaning of Section 34 of the Act;
 - (d) The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;
 - (e) The right to prevent any transmission or disclosure of any sensitive health related data that is likely to cause damage or distress to the owner;
 - (f) The right not to be refused health service, if they refuse to consent to generation, collection, storage, transmission and disclosure of their health data;
 - (g) The right to seek compensation for damages caused by a breach of digital health data.

29. Purposes of collection, storage, transmission and use of the digital health data

- (1) Digital health data may be generated, collected, stored, and transmitted by a clinical establishment and; collected, stored and transmitted by health information exchange, for the following purposes:
 - (a) To advance the delivery of 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 undertake academic research and other related purposes

Provided that personally identifiable information may only be used for the purposes of direct care of the owner of the data, as specified in clauses (a) to (c) of sub-section (1), subject to provisions of section 28, to the extent considered necessary, and in the best interest of the owner

Provided further that for public health related purposes mentioned in clauses (d) to (h) of sub-section (1), only de-identified or anonymized data shall be used, in the manner as may be prescribed under this Act.

- (2) Digital health data may be generated, collected, and stored by any other entity for the purposes mentioned in clauses (a) to (c) of Sub-Section (1).
- (3) Digital health data shall not be used for any other purpose, except in accordance with the provisions of this Act.

Provided that the digital health data shall be used only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to use the information.

- (4) There shall be no access to, or disclosure of personally identifiable information, except in accordance with the provisions of this Act.

Provided that the digital health data shall be accessed or disclosed only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to access or disclose the information.

- (5) Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government.

Explanation: Insurance companies shall not insist on accessing the digital health data of persons who seek to purchase health insurance policies or during the processing of any insurance claim.

Provided that for the purpose of processing of insurance claims, the insurance company shall seek consent from the owner to seek access his or her digital health data from the clinical establishment to which the claim relates

30. Collection of health data

- (1) No health data shall be collected, for the purposes of conversion to digital health data, by any clinical establishment, or any other entity in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may, by consent from the owner, recorded in the form and manner as may be prescribed under this Act, lawfully collect the required health data, after informing the owner of the following:

- (a) The rights of the owner as laid down in this Act, including the right to refusal to give consent to the generation and collection of such data;
 - (b) The purpose of collection of such health data;
 - (c) The identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format;
 - (d) The identity of the recipients who may have access to such digital health data on a need to know basis
- (3) A clinical establishment or any other entity, shall furnish a copy of the consent form to the owner.
 - (4) Any other entity that collects any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data.
 - (5) Without prejudice to the above sub-section (2), when an individual is incapacitated or incompetent to provide consent, either due to physical or mental incapacity, the clinical establishment may collect health data by obtaining proxy consent from a nominated representative, relative, care giver or such other person, as may be prescribed under this Act, and who has the legal capacity to consent.

Provided that where the individual has regained his or her capacity to give or refuse consent for the collection of his or her health data by the clinical establishment, he or she shall have the option to seek withdrawal of proxy consent and obtaining his or her own consent for collection of such health data, in such form and manner as may be prescribed by the National Electronic Health Authority of India.

- (6) Where a person is a minor and it is in the best interest of the minor, proxy consent can be obtained by the minor's legal guardian, or representative.

Provided that upon attaining majority, the minor shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.

31. Ownership of digital health data

- (1) The digital health data generated, collected, stored or transmitted shall be owned by the individual whose health data has been digitised;
- (2) A clinical establishment or Health Information Exchange shall hold such digital health care data referred to in sub-section (1) above in trust for the owner;
- (3) Any other entity who is in custody of any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data;
- (4) Notwithstanding anything stated in the above sub-sections (1) to (3), the medium of storage and transmission of digital health data shall be

owned by the clinical establishment or health information exchange, as the case may be.

32. Storing of digital health data

- (1) No digital health data shall be stored by any clinical establishment or entity or health information exchange in any manner, except in accordance with the provisions of this Act.
- (2) The clinical establishment or health information exchange, as the case may be, shall hold all digital health data, on behalf of National Electronic Health Authority; and such data be used for such purposes as stated in Section 29, without compromising the privacy or confidentiality of the owner, and security of such data.
- (3) The digital health data vested with the National Electronic Health Authority as per sub-section 2 above, shall be stored and may be transmitted or used in such form and manner as may be prescribed by the National Electronic Health Authority.

33. Transmission of data

- (1) No digital health data shall be transmitted by a clinical establishment or health information exchange, or any other entity, as the case may be, in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may transmit the digital health data to the health information exchange securely, in an encrypted form, after retaining a copy for reasonable use by the clinical establishment.

Provided that for such secure, encrypted and instantaneous transmission of digital health data as referred in sub-section (2), the National Electronic Health Authority of India shall prescribe appropriate standards for physical, administrative and technical measures, keeping in mind the privacy and confidentiality of the owner, by notification

- (3) The digital health data shall be transmitted by a clinical establishment or entity or health information exchange only upon the consent of the owner, after being informed of the rights of the owner under Section 28, and the specific purposes of collection of such data under Section 29.
- (4) A health information exchange shall maintain a register in such form and manner as may be prescribed by the Central Government, containing all details of the transmission of the digital health data between a clinical establishment and health information exchange, and between health information exchanges *inter se*.

34. Access to digital health data

- (1) No digital health data collected, stored or transmitted by a clinical establishment or health information exchange, as the case may be,

shall be accessed by any person, except in accordance with the provisions of this Act.

- (2) The digital health data collected or stored or transmitted by a clinical establishment or health information exchange, as the case may be, may be accessed by the clinical establishment, on a need to know basis, in such form and manner as may be prescribed under this Act.
- (3) The government departments through their respective Secretaries, may submit request for digital health data in de-identified/anonymized form, to the National Electronic Health Authority, in the form and manner specified by the Authority, subject to provisions of clauses (d) to (h) of sub-section (1) of section 29 of this act.

Provided that the National Electronic Health Authority of India may prescribe any other class of persons who may access digital health data, which is anonymized, for the purposes stated in clause (d) to (h) of sub-section (1) of section 29 of the Act.

- (4) In case where access to digital health data is necessary for the purpose of investigation into cognizable offences, or for administration of justice, such access may be granted to an investigating authority only with the order of the competent court;
- (5) The owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Electronic Health Authority of India.
- (6) In case of an emergency, certain digital health data shall be immediately made accessible to a clinical establishment, upon a request, including information related to allergies, drug interactions and such other information as may be specified;
- (7) In case of an emergency, the relatives of the owner may have access to such data for the purpose of correct treatment of the owner, subject to such conditions as may be prescribed under this Act.
- (8) In case of death of the owner of digital health data, the legal heirs or representative of such owner may have access to such data, only upon the application of such heirs or representatives in such form and manner as may be specified by the National Electronic Health Authority of India.

Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner.

Provided further that in case of death of the owner, the National Electronic Health Authority, shall use the digital health data only in anonymized form.

- (9) All clinical establishments and health information exchanges shall maintain a register in a digital form to record the purposes and usage of digital health data accessed within the meaning of this Section, in such form and manner, as may be specified by the National Electronic Health Authority.

35. Duty to maintain privacy and confidentiality of digital health data

- (10)
- (1) A clinical establishment, health information exchange, State Electronic Health Authority and the National Electronic Health Authority, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner;
 - (2) Any other entity, which has generated and collected digital health data, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner.
 - (3) The privacy, confidentiality and security of digital health data shall be ensured by taking all necessary physical, administrative and technical measures, that may be prescribed or specified, to ensure that the digital health data, collected, stored and transmitted by them, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.
 - (4) Without prejudice to the above provisions, a clinical establishment or health information exchange shall ensure through regular training and oversight that their personnel comply with the security protocols and procedures as may be prescribed or specified under this act.
 - (5) A clinical establishment, or a health information exchange, shall provide notice immediately, and in all circumstances not later than three working days to the owner, in such manner as may be prescribed under this Act, in case of any breach or serious breach of such digital health data.

36. Procedure for rectification of digital health data

- (1) An owner of the digital health data shall seek for rectifying the incorrect digital health data stored in any clinical establishment or health information exchange, as the case may be, by making an application in such form and manner as may be prescribed under this Act.
- (2) On receipt of such application under sub section (1), the clinical establishment or health information exchange shall rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.

**CHAPTER V
OFFENCES AND PENALTIES**

37. Breach of digital health data

- (1) Digital health data is said to be breached, if:
 - (a) any person generates, collects, stores, transmits or discloses digital health information in contravention to the provisions of Chapter II of this Act; or

- (b) Any person does anything in contravention of the exclusive right conferred upon the owner of the digital health data; or
 - (c) Digital health data collected, stored or transmitted by any person is not secured as per the standards prescribed by the Act or any rules thereunder; or
 - (d) Any person damages, destroys, deletes, affects injuriously by any means or tampers with any digital health data.
- (2) Any person who breaches digital health data shall be liable to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place.

38. Serious breach of digital health data:

- (1) A serious digital health data breach shall be said to have taken place, if:
- (a) A person commits a breach of digital health data intentionally, dishonestly, fraudulently or negligently; or
 - (b) Any breach of digital health data occurs, which relates to information which is not anonymised or de-identified; or
 - (c) A breach of digital health data occurs where a person failed to secure the data as per the standards prescribed by the Act or any rules thereunder; or
 - (d) Any person uses the digital health data for commercial purposes or commercial gain; or
 - (e) An entity, clinical establishment or health information exchange commits breach of digital health data repeatedly;

Explanation: The terms “dishonestly” and “fraudulently” shall have the same meaning as assigned to them under the Indian Penal Code, 1860

- (2) Any person who commits a serious breach of health care data shall be punished with imprisonment, which shall extend from three years and up to five years; or fine, which shall not be less than five lakh of rupees.

Provided that, any fine imposed as part of sub-section (2) may be provided to the individual whose data is breached, by the Court, as it deems fit as compensation.

39. Compensation for serious breach of digital health information

- (1) A person or an entity committing a serious breach of digital health information shall be liable to pay damages by way of compensation to the owner of the digital health data in relation to which the breach took place.
- (2) Where any compensation has been awarded under sub-section (2) of section 37, it shall be taken into account when determining the claim made by the person affected.

40. Penalty for failure to furnish information, return or failure to observe rules and directions, etc.,

- (1) If any person required under this Act or any rules made thereunder, fails to furnish any information or document or books or returns or reports etc., within the time specified, to National Electronic Health Authority, or the State Electronic Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (2) Any person required under this Act or any rules made thereunder fails to comply, within the time specified, with directions issued by the National Electronic Health Authority, or the State Electronic Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (3) Any person which is required under this Act or any rules made thereunder, after having been called upon by the National Electronic Health Authority in writing, or the State Electronic Health Authority, as the case may be, to redress the grievances of owners of digital healthcare data, fails to redress such grievances within the time specified, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees.

41. Obtaining the digital health information of another person

Whoever, fraudulently or dishonestly, obtains the digital health information of another person, which he is not entitled to obtain under the Act from a person or entity storing such information shall be punished with imprisonment for a term which shall extend up to one year or fine, which shall be not less than one lakh rupees; or both.

42. Data theft

Whoever intentionally and without authorization acquires or accesses any digital health data shall be punished with imprisonment for a term, which shall extend from three years up to five years or fine, which shall be not less than five lakh rupees; or both.

43. Cognizance of offences by court

- (1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made thereunder, save on complaint made by the Central Government, State Government, the National Electronic Health Authority of India, State Electronic Health Authority, or a person affected.
- (2) No Court inferior to that of a Court of Sessions shall try any offence punishable under sections 38, 41 and 42 of this Act.

44. Offences by companies

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time when the contravention was committed, was in charge of and was responsible to the company, for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the contravention, and shall be liable to be proceeded against and punished accordingly.

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the commission of such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer of the company shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation 1.— For the purpose of this Section –

- (a) “company” means any body corporate and includes a clinical establishment, entity, firm or other association of individuals; and
- (b) “director” in relation to
- (i) a firm, means a partner in the firm;
 - (ii) any association of persons or a body of individuals, means any member controlling the affairs thereof;

Explanation 2.— For the removal of doubts it is hereby clarified that a company may be prosecuted notwithstanding that the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual.

CHAPTER VI CENTRAL AND STATE ADJUDICATING AUTHORITIES

45. Complaints to State Adjudicating Authority

- (1) For any breach of digital health data by a clinical establishment or any entity an aggrieved person or owner may complain to the State Adjudicatory Authority in writing as may be prescribed, and seek

reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;

- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (2) or (3) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the State Electronic Health Authority under section 40 of this act, may prefer an appeal to the State Adjudicating Authority within a period of forty-five days from the date on which a copy of the order is received.

46. Complaints to the Central Adjudicating Authority

- (1) For any breach of digital health data by a health information exchange or State Electronic Health Authority or the National Electronic Health Authority of India, an aggrieved person or owner may complain to the Central Adjudicatory Authority in writing as may be prescribed, and seek reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;
- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (3) or (4) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the National Electronic Health Authority under section 40 of this act, may prefer an appeal to the Central Adjudicating Authority under this Act within a period of forty-five days from the date on which a copy of the order is received.
- (6) Any person or entity or owner or State Electronic Health Authority, aggrieved by the order of the State Adjudicatory Authority may prefer an appeal to the Central Adjudicatory Authority, within 3 months from the date on which a copy of the order is received.

47. Adjudicating authorities, composition, powers etc.

- (1) The Central Government shall by Notification, appoint a Central Adjudicating Authority, and the State Governments shall by notification,

- appoint State Adjudication Authorities respectively, to exercise jurisdiction, powers and authority conferred by or under this Act
- (2) The Adjudicating Authority, whether Central or State, shall consist of a Chairperson and two other members, provided that at least one of such persons shall be from the field of law.
 - (3) A person shall, however, not be qualified for appointment as Member of an Adjudicating Authority –
 - (a) In the field of law, unless he:
 - (i) Is qualified for appointment as District Judge; or
 - (ii) Has been a member of the Indian Legal Service and has held a post in Grade I of the service;
 - (b) In the field of medicine, information (health) science or administration, unless he possesses such qualifications as may be prescribed by the Central Government.
 - (4) The Central Government and the State Governments shall appoint the Member from the field of law, to be the Chairperson of the Central Adjudicating Authority and State Adjudicatory Authorities respectively.
 - (5) Subject to the provisions of this Act,
 - (a) The Central Adjudicatory Authority shall sit at New Delhi...
 - (b) The State Adjudicating Authorities shall ordinarily sit at the State Capitals;
 - (6) The Chairperson and every Member shall hold office as such for a term of five years from the date on which he enters upon his office.

Provided that no Chairperson or other Member shall hold office as such after he has attained the age of sixty-five years.

- (7) The salary and allowances payable and other terms and conditions of service of the Members shall be such as may be prescribed.

Provided that neither the salary or allowances nor the other terms and conditions of service of the Member shall be varied to his disadvantage after appointment.

- (8) If, for any reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government or the State Governments, as the case may be, shall appoint another person in accordance with the provisions of this Act to fill the vacancy, and the proceedings may be continued before the Adjudicating Authority from the stage at which the vacancy is filled.
- (9) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government or the State Government, as the case may be, resign his office:

Provided that, the Chairperson or any other Member shall, unless he is permitted by the Central or State Government to relinquish his office sooner, continue to hold office until the expiry of the three months from the date of receipt of such notice or until a person duly appointed as his

successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- (10) The Chairperson or any other Member shall not be removed from his office except by an order made by the Central Government or the State Government, as the case may be, after giving necessary opportunity of being heard.
- (11) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior-most Member shall act as the Chairperson of the Adjudicating Authority until the date on which a new Chairperson appointed in accordance with the provisions of this act to fill such vacancy, enters upon his office.
- (12) When the Chairperson of the Adjudicating Authority is unable to discharge his functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson of the Adjudicating Authority until the date on which the Chairperson of the Adjudicating Authority resumes his duties.
- (13) The Adjudicating Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Adjudicating Authority shall have powers to regulate its own procedure.

48. Staff of the adjudicating authority

- (1) The Central Government shall provide the Central Adjudicating Authority, and the State Governments shall provide the State Adjudicating Authorities, with such officers and employees as it may think fit.
- (2) The officers and employees of the Adjudicating Authority shall discharge their functions under the general superintendence of the Chairperson of the Adjudicating Authority.
- (3) The salaries and allowances and other conditions of service of the office and employees of the Adjudicating Authority shall be such as may be prescribed.

49. Power regarding summons, production of documents and evidence

- (1) The Central Adjudicating Authority and State Adjudicatory Authorities shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint in respect of the following matters, namely
 - (a) Discovery and inspection;
 - (b) Enforcing the attendance of any person, including any officer of a Clinical establishment or a health information exchange and examining him on oath;
 - (c) Compelling the production of records;
 - (d) Receiving evidence on affidavits;

- (e) Issuing commissions for examination of witnesses and documents; and
 - (f) Any other matter which may be prescribed by the Central Government.
- (2) All persons so summoned shall be bound to attend in person or through authorized agents, as the Adjudicating Authority may direct, and shall be bound to state the truth upon any subject respecting which they are examined or make statements, and produce such documents as may be required.
- (3) Every proceeding under this section shall be deemed to be a judicial proceeding within the meaning of Section 193 and Section 228 of the Indian Penal Code (45 of 1860).

50. Civil court not to have jurisdiction

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Central Adjudicatory Authority or the State Adjudicatory Authority is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

51. Appeal to High Court

- (1) Any person aggrieved by any decision or order of the Central Adjudicatory Authority may file an appeal to the High Court within sixty-days from the date of communication of the decision or order of the Adjudicatory Authority to him on any question of law or fact arising out of such order.
- (2) Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

CHAPTER VII
MISCELLANEOUS PROVISIONS

52. Act to supersede any other law

- (1) The provisions of this Act shall be taken to supersede any other law for the time being in force with respect to digital medical record, digital health record or digital personal/protected health information which is being referred to as 'digital health data' hereunder.

53. Power of the Central Government to make rules

- (1) The Central Government may, by notification in the Official Gazette, make rules for the purposes of carrying out the provisions of this Act.

- (2) Every Rule made by the Central government under this Act shall be laid, as soon as may be after it is made, before each House of Parliament.

54. Power of the State Government to make Rules –


- (1) Subject to the other provisions of this Act, the State Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act;
- (2) Every Rule made by the State government under this Act shall as soon as may be after its made, be placed in each House of the State Legislature, where there are two houses.

55. Removal of difficulty by the government

- (1) This Act shall be applied and construed to effectuate its general purpose to facilitate uniformity of the law/s with respect to the subject matters of this Act among all the States.
- (2) Notwithstanding the above, this Act does not restrict or limit the rights and obligations under any of the State laws or regulations, so long as the rights and obligations enumerated herein are fully complied with.
- (3) In the event of a conflict between this Act and other State or local laws or regulations, or administrative procedures, the provisions of this Act shall apply. However, the existing laws, rules and regulations, at national and State levels, shall continue to prevail to the extent of consistency with this Act and only portions thereof shall become severable and unenforceable to the extent of inconsistency with any provision of this Act.
- (4) The provisions of this Act are severable such that if any provision of this Act or its application to any person or circumstances is held invalid judicially, the invalidity shall not affect other provisions or applications of this Act which can be given effect to without the particular invalid provision or application.
- (5) Notwithstanding the above, the Governments shall undertake a comprehensive review of all the laws or provisions of laws related to health within 1 year of this Act coming into force for their compatibility with this Act.

Schedule I

Personally Identifiable Information

- (iv) Name
 - (v) Address
 - (vi) Date of Birth
 - (vii) Telephone Number
 - (viii) Email Address
 - (ix) Password
 - (x) Financial information such as bank account or credit card or debit card or other payment instrument details;
 - (xi) Physical, physiological and mental health condition;
 - (xii) Sexual orientation;
 - (xiii) Medical records and history;
 - (xiv) Biometric Information;
 - (xv) Vehicle number
 - (xvi) Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL').
- 

New Issue – we should not disallow direct sharing of identifiable data for direct patient care between two hospitals.