Comments on the Draft Digital Information Security in Healthcare Act

Shweta Mohandas and Amber Sinha
The Centre for Internet and Society
April 21, 2018

I. Preliminary

This submission presents comments by the Centre for Internet and Society, India ("CIS") on the Draft Digital Information Security in Healthcare Act, released by Ministry of Health & Family Welfare, Government of India. CIS has conducted research on the issues of privacy, data protection and data security since 2010 and is thankful for the opportunity to put forth its views. This submission was made on April 21, 2018.

II. About CIS

CIS is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, freedom of speech and expression, intermediary liability, digital privacy, and cybersecurity.

CIS has conducted extensive research into the areas privacy, data protection, data security, and was also a member of the Committee of Experts constituted under Justice A P Shah.[1] CIS values the fundamental principles of justice, equality, freedom and economic development. This submission is consistent with CIS' commitment to these values, the safeguarding of general public interest and the protection of individuals' right to privacy and data protection. Accordingly, the comments in this submission aim to further these principles.

III. General Comments

The digitization of health records, adoption of national standards for electronic health records and use of healthcare data for research represents a significant public interest opportunity for Digital India. We note with appreciation the privacy and security provisions in the Draft Digital Information Security in Healthcare Act. However, as we await the recommendations from the Justice Srikrishna Committee towards the creation of a data protection law in India, we feel it is important the different government ministries and departments to have clear coordination, to ensure consistency and convergence across the different sectoral laws address privacy issues.

[1] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

Privacy Safeguards

However, the draft legislation does not contain provisions for instances where the digital health data of the owner has been collected without his/her consent, neither does it mention the status of the data when the owner withdraws their consent. The draft states that the data can be withdrawn by the owner but it does not state the manner in which the data will be deleted from the records and/or if any copy would be maintained as a record by the custodian of the data. There are also issues with respect to the right to privacy and its violation thereof due to the non-consensual collection of health data.This is an issue which needs to be addressed in this draft legislation. It should not be left unaddressed as this would only result in a lack of clarity which would require protracted court cases to resolve.

Presently, the proposed draft legislation is being introduced without comprehensive privacy safeguards in place on issues such as consent, collection, and retention of data. Though the National Electronic Health Authority is responsible for safeguarding the privacy, security, and confidentiality of the digital health data of the owner (Section 35(1)) - it is not adequate given the fact that India does not have a comprehensive privacy legislation. Though section 43A and associated Rules of the Information Technology Act would apply to the collection, use, and sharing of digital health data by the National and State Electronic Health Authority as well as clinical establishments and other entities (as they would fall under the definition of ‘body corporate’ under the IT Act), the Health Information Exchange would not clearly be body corporate as per the IT Act and would not fall under the ambit of the Acts provisions or Rules. Safeguards are needed to protect against the invasion of informational privacy and physical privacy at the level of these controlled bodies which are controlled by the National Electronic Health Authority.

Annual Public Reporting

The draft legislation does not require the National or even the State Electronic Health Authority to disclose publicly available information on an annual basis regarding the functioning and financial aspects of matters contained within the draft legislation. Such disclosure is crucial to ensure that the public is able to make informed decisions. Categories that could be included in such reports include: Number of digital health records added, total number of records contained in the database, number of records deleted from the database, the number of health information exchanges established, the number of records that are transmitted internationally, and the number of data breaches, to name a few.

IV. Specific Comments

A. Stated Aims and Objectives

As stated, the Digital Information Security in Healthcare Act provides 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. As stated, the purpose of the Digital Information Security in Healthcare Act is to facilitate the establishment of the National and State Electronic Health Authorities and Health Information Exchanges, that are incharge of standardising and regulating the process of data collection, storage and transmission. This part of the draft legislation fails to mention that the it also prescribes the formation of a National Executive Committee and a State Executive Committee.

Furthermore, the draft legislation contains provisions beyond its stated purpose. These include:

a) The function of the National Electronic Health Authority to “lay down the protocol for transmission of digital health data to and receiving it from other countries”. (Section 22(1)(e))

b) The establishment of the Central and State Adjudicatory Authority for the purpose for adjudicating over complaints regarding the breach of digital health data (Section 45 and 46).

Recommendation: The stated purpose of the draft legislation should mention the formation of the National and State Executive Committee as well as the Central and State Adjudicatory Authority. The stated purpose of the draft legislation should inform the reader that it contains the rights of the data owner as well as address other relevant aspects of the draft legislation.

B. Section 2

Section 2 explains the commencement and application of the Act.

Comments: This section states that different dates may be appointed for different states and different provisions of the draft legislation. This leaves the effective commencement of the Act in ambiguity, if the Act is not uniformly applied in India the question of portability and use of digital health data will be ineffective. With

regard to the statement that different portions of the draft legislation might come into force on different dates, this might cause some compromise on the security and privacy of the digital health data of the owner.

Recommendations: It can be understood that different states in India are in varying stages of digitization. For this reason, the draft legislation might not be effective if applied, although implementing the draft legislation in all the States at once would help in cases of patients moving from one state to another. The provisions of the draft legislation need to be effective uniformly to reduce confusion as well as to ensure that the data, privacy and security of the people are not compromised.

C. Section 3

Section 3 defines the terms used in the draft legislation

Comments: Some of the terms are incomplete and a few of the terms used in the draft legislation have not been included in the list of definitions.

Recommendations: The term ‘direct care’ needs to be defined. The term is first used in the proviso to Section 29, which states “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.” It is crucial that the draft legislation defines direct care especially when it is with respect to the use of personally identifiable information.

The term ‘Health Information Exchange’ as defined under Section 2(1)(h) is vague and it does not clearly explain the body formed under this draft legislation. Section 19 of the draft legislation states that the central government shall establish health information exchanges; and the following section 20 and 21 deal with the management of the exchanges and the powers and functions of the Chief Information Executive. The draft legislation fails to state what the Health Information Exchange is, and as various provisions of the draft legislation group clinical establishments and health information exchanges together, there needs to be a more detailed definition of it.

In the definition of ‘Clinical Establishments’ under Section 3(1)(i) it is stated as follows “but does that include clinical establishments owned, controlled or managed by the Armed Forces”.There seems to be a typographical error and the part should read as “but does not include clinical establishments owned,

controlled or managed by the Armed Forces". As the use of the word 'but' suggests an exception, it needs to be made clarified so as to remove ambiguity.

The term "De-identification" that is defined in Section 3(1)(d) is not used anywhere outside the definitions clause and should be removed.

D. Section 5

This provision addresses the composition of the National Electronic Health Authority Of India.

Comment: The National Electronic Health Authority is the apex body that is responsible for not only setting standards and protocols for the generation, collection, storage and transmission of the digital health data, but also to ensure that steps are taken to maintain the privacy and security of the data. However in the composition of the Authority there is no member who specialises in security, or a Chief Security Officer.

Recommendations: One of the primary objectives of the Authority is to safeguard the privacy and security of the data. For this reason there needs to be an officer appointed specifically to advise and decide on strategies to improve privacy and security. For example Section 3001 of the (American) Health Information Technology for Economic and Clinical Health draft legislation'' (HITECH Act) of provides for the appointment of a Chief Privacy Officer whose duty is to advise the National Coordinator on privacy, security, and data stewardship of electronic health information.

E. Section 6

Section 6 addresses the composition of the National Executive Committee

Comments: With regard to the composition of the of the committee members, Section 6(1)(d) states that the Committee shall be 'supported by consultants and ehealth section.'This sentence is vague as well as the number of consultants that are to be appointed is not mentioned.

Recommendations: This section should clarify what 'e-health section' is and define it in case this entity has been formed for the purposes of this draft legislation. The number of consultants also needs to be stated. If not a precise number, the section should state the upper limit to the number of consultants that can be appointed.

F. Section 8

Section 8 lays down the composition of the State Electronic Health Authorities

Comments: Regarding the composition of the State Electronic Health Authorities, Section 8(1)(d) specifies the appointment of three ex-officio members. This clause states that the three ex-officio members to be appointed by the State Government should be from the 'Director, State Health Services; from the State Information Technology department; and from the State Law department.The composition of this authority is different from the National Authority. The National Authority comprised of four ex officio members the addition being a representative from the Ministry of Panchayati Raj or Ministry of Women & Child Development. This representative is missing from the State Electronic Health Authority.

Recommendations: There needs to be representation ideally from both the local government bodies and also from members who have worked on issues relating to women and children. This representation is required to ensure a more diverse set of expertise in looking at various issues that might arise with respect to digital health records.

G. Section 9

Section 9 addresses details of the formation and composition of the State Executive Committee

Comments: In the composition of the of the Committee members, Section 9(1)(d) states that the Committee shall be 'supported by consultants and ehealth section.' This term is vague as well as the number of consultants that are to be appointed is not mentioned.

Recommendations: This section should clarify what 'e-health section' means as well as define a number of such consultants that are to be appointed by the Committee.

H. Section 16

Section 16 explains the disqualifications of the members of the National Electronic Health Authority or a State Electronic Health Authority.

Comments: In Section 16(1)(ii) the clause stipulating the disqualification of the members reads as follows “Is an undercharged insolvent”.This seems to look like an typographical error.

Recommendations: The clause should read as “is an undischarged insolvent, as can be seen from other legislations that have provisions that detail disqualifications criterias. For example in the Consumer Protection Act in the composition of the District Forum (Section 10(1)(iii)(a) states that the member of the District Forum shall be disqualified as a member if he is an “is an undischarged insolvent”. Section 16(1)(ii) of the Act should be edited accordingly, though if the clause is meant to read as stated the Act should provide a definition of the term.

I. Section 21

Section 21 explains the appointment of The Chief Health Information Executive and his functions.

Comments: Section 21(2)(b) states that the Chief Health Information Executive (CHIE) is the data controlling authority of the health information exchange and is responsible for the smooth functioning of the exchange. In order to ensure this, the CHIE has the power to access and process the digital health data that is transmitted by the clinical establishments, for the transmission of the digital health care data. Although the draft legislation states that theses powers will be according to the norms prescribed by the National Electronic Health Authority of India, until these norms are introduced the CHIE will be accessing the data.

Recommendations: The norms relating to the functioning of the CHIE, his powers and functions must be formulated at the earliest.

J. Section 22

Section 22 explains the delegation of powers and functions to the National Electronic Health Authority of India.

Comments: This section delegates a number of functions to the Authority that places it in the role of a manager and regulator for issues pertaining to digital health data including periodically overseeing the functioning of the health information exchanges etc.

Recommendations: The functions of the Board should be limited to developing standards and protocols, safeguarding privacy and other rights, ensuring public transparency, promoting information and debate and a few other limited functions

necessary for a regulatory authority. Towards this, the Board should be comprised of separate Committees to address these different functions. At the minimum, there should be a Committee to oversee the workings of the health information exchanges as well as one to handel breaches in security.

K. Section 28

Section 28 lays down the rights of the owner of the digital health data. Section 28 (1)(e) states that the data owner has the right to prevent any transmission or disclosure of any ‘sensitive health related data’. The term sensitive health related data has not been defined under the draft legislation, however the draft legislation defines sensitive health related information under Section 3(1)(o).

Recommendation: This clause should read as “ The right to prevent any transmission or disclosure of any ‘sensitive health related information’ that is likely to cause damage or distress to the owner.

L. Section 28(7)

Section 28 (7) of the draft legislation states that 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.

Comments: The draft legislation fails to explain how the data can be accessed by the data owner, through an online portal, an app, data centers etc. The draft legislation also lacks a provision that ensures that a copy of the digital health data is provided to every data owner.

Recommendations: The draft legislation should specifically state how the data can be accessed by the data owner. Additionally the owner of the data must be provided with a copy of his healthcare data. Either in a printed format or available online for download.This is a necessary right of the owner of the data. This helps in making informed decisions regarding the use of data as well holds the data custodian accountable. This also helps in tracking errors in a person's records.This data should also be available within a prescribed time.

M. Section 37

Section 37 discusses the breach of digital health data

Comments: This section while stating what qualifies as a breach of digital health data as well as the punishment for the same fails to mention the measures that

are to be taken once the breach is detected as well as the measures to mitigate the breach. Section 21(2)(d) states that the Chief Health Information Executive has to notify the data breach to the owner and 'such other concerned' and Section 35(5) also states that the clinical establishment or a health information exchange shall inform the owner of the data of the breach immediately and not later than three working days. However the draft legislation does not explicitly state that the breach has to be notified to the apex bodies i.e the Stta and Neha.

Recommendations: This section should also specify that the breach will be notified to the apex bodies immediately as well as lay down step for control and mitigation of the breach. For example, HIPAA breach notification rule states that "If Public Health Information(PHI) is disclosed in violation of its policies and procedures, a covered entity must mitigate, to the furthest extent actionable, any harmful effects." Additionally HIPAA also requires that in case of a breach the health care provider has to notify the Secretary of Health and Human Services. It also states that if a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. As breaches such as cyber attacks do not happen in isolation and can affect a number of centres at once, this requirement helps individuals know that there has been a breach as well as help keep the data custodians accountable.

N. Sections 45 and 46

These provisions deal with the complaints to the State Adjudicating Authority and the Central Adjudicating Authority respectively.

Comment: While these two sections provide for recourse that the data owner can take in case of any breach of his data. Some of the provisions are limited, for example the complaints can only be made on account of a breach of digital health data. This fails to consider complaints that might not come under the definition of breach under the draft legislation. These can be for example, the refusal to provide digital healthcare information, the failure to remove records after withdrawal of consent etc. Although Section 37(1)(b) includes anything done in contravention of the exclusive right conferred upon the owner of the digital health data as a breach.

Recommendations: This section should lay down in detail the issues which the data owner can seek redressal from and not limit its scope only to breaches.