INDIAN MEDICAL ASSOCIATION, PUNE BRANCH

Dr. Nitu Mandke IMA House, 992, Shukrawar Peth, Tilak Rd., Pune - 411 002.
Email : imaofpune@gmail.com Website : www.imapune.com
Telephone : 020 - 24430042 / 24464771 Office Hours : 11am to 6pm

Helping Hands
2018 - 19

Theme : Helping Hands

President	Hon. Secretaries		Hon. Treasurer
Dr. Padma Iyer	Dr. Rajkumar Shah	Dr. Meenakshi Deshpande	Dr. B. L. Deshmukh
9373305154	9422500666	9922464365	9960172759

Imm. Past President	President Elect	Vice President	Jt. Hon. Secretary	Asst. Sec. & Jt. Treasurer
Dr. Prakash Marathe	Dr. Sanjay Patil	Dr. Aarti Nimkar	Dr. Raju Varyani	Dr. Rajan Sancheti
9823071292	9822520257	9822304882	9822646025	9823147882

IMA/PN/GEN/2018-19/37

Date : 16/04/2018

Mr S. C. Rajeev, Director (eHealth)
Phn No. 23062205, eHealth Section,
Ministry of Health and Family Welfare,
Room No 211-D, Nirman Bhavan,
New Delhi 110108

Dear Sir,

With reference to your notice dt 21st March 2018, inviting comments / views on the draft of the Digital Information Security in Healthcare, Act (2018); Indian Medical Association, Pune is pleased to submit herewith comments compiled after thorough discussion of members of medico-legal cell.

If any clarification is required, please feel free to contact Dr. Rajeev Joshi on 9822084614.

With warm regards,

Dr. Jayant Navarangé,
Chairman, Medico-legal Cell
IMA, Pune

Dr. Rajeev Joshi
Chairman, eCommunication cell
IMA, Pune

Dr. Sanjay Patil,
Chairman, Hospital Board of India
Pune Subchapter, IMA

Dr. Padma Iyer,
President, IMA Pune

Dr. Rajkumar Shah / Dr. Meenakshi Deshpande
Hon. Secretaries, Indian Medical Association, Pune

Encl:
Comments of Indian Medical Association, Pune on DISHA Act (2018)

Comments from Indian Medical Association, Pune
on
Digital Information Security in Healthcare Act

Abbreviations:
CE: Clinical establishment i.e. doctor, hospital, laboratory, pharmacists etc.
HIE: Health information exchange.
Term "Owner of data" (used in act) is used interchangeably with patient (in comments) as per convenience

General comments: This act is premature, i.e. before any clarity on use of Aadhar Number for indexing the digital health data, of every citizen of country. Without Aadhar, it would be difficult to exchange health data. Most of the population does not have PAN number and 40% do not have voter ID. Children below 18 years do not have driving license. Only Aadhar has potential to be used as secondary index, in electronic health record generated by Clinical Establishments (CE). Aadhar can be used as primary index by HIE.

Purpose of Health Information Exchange is twofold. One is to create longitudinal health record of individual patient with which patient will be benefitted. Second is to create cross-sectional health database from which public health decisions can be taken based on actionable intelligence. It should be noted that CEs per say will not be benefitted in both above scenarios, and have nothing to lose if they do not transmit data to HIE.

Current scenario in digitization of healthcare data should be considered before implementation of this act. Whether MOH&FW wants to encourage use of information technology (IT) in healthcare or not; is a basic question which needs to be answered. Currently most of the use of IT in CE is for administrative tasks as well as billing, whereas MOH&FW would be benefitted if clinical information is accumulated and sent to HIE.

Healthcare professionals are duty bound to ensure confidentiality of information given to them by the patients. For 70 years since independence, we have seen very few cases of breach of confidentiality when the medical records are on paper (e.g. Mr. X Vs Hospital Z). Software glitches and hackers are more likely to be responsible for breach of digital health data. Holding CEs and medical professionals responsible for the same will not be acceptable. CEs will make it a point not to transmit data to HIE, as chances of leak are more at HIE than CE, and this will defeat whole purpose of health information exchange. Breach of confidentiality from CE should be tried under medical council act. Breach of security from HIE should be tried under this act.

To encourage digitization of health data, MOH&FW should recommend some tax benefits for investment in IT infrastructure in CE to support HIE. Act should have some penal provisions if digital data is generated but not transmitted to HIE. Risk of breach of digital health data should be weighed with benefits community will have from actionable intelligence. Government should take responsibility of data security as the HIEs will be operated mostly by government machinery rather than Clinical Establishments.

The CEs will suffer tremendously if DISHA act is implemented in its present form. Our experience with PCPNDT and Clinical Establishment Act is not good. The question "why does the Indian govt. treat doctors as potential criminals?" needs to be answered squarely. Members of medical fraternity must put forward their views and get some provisions amended before the act is passed.

Indian Medical Council Act, 1956 mandate physician-patient confidentiality unless the disclosure of the patient s information is required by law, or if there is a serious and identified risk to an individual / community, or the disease is a notifiable one.

The Clinical Establishments Rules, 2012 requires CEs to maintain and provide Electronic Medical Records / Electronic Health Records, thus mandating the storage of health information in an electronic format. While the government can force CEs to collect digital health data, it cannot force them to transmit it except for notifiable diseases. Therefore, initially transmission should be limited to notifiable diseases only.

IMC Code requires that the patient, her relatives and responsible friends have knowledge of the patient's condition so as to serve her best interests, thus allowing for disclosure without the consent of the patient. Further, physicians are encouraged to computerize medical records, maintain them for a period of three years and provide access to them to the patient upon her request. Therefore, Indian Medical Council act encourages "transmission" of information to friends and relatives, but current DISHA act prevents such transmission of information without explicit consent from patient. These ambiguities need to be addressed.

Point wise comments:

Clauses in act	Comments from Indian Medical Association, Pune
28(8)(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;	Patient should notify the CE, with copy to HIE, regarding inaccuracies or incompleteness of the health data; which CE should rectify within stipulated time. IF CE fails to rectify, then HIE should rectify the data.
28(8) (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;	Is the consent to be taken once at the time or registration, or at the time of each encounter? Whether the consent should be on paper, signed by patient and his relative or electronic? Should the consent also include permission to HIE to allow access to information by another CE?
28(8)(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;	Whether the HIE will send notification on patients mobile / email to patients email ID?
28(8)(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;	Whether the CE has to confirm identity and relationship of the family members as per definition in 3(1)(m) before sharing the digital health data? Why this responsibility should not be entrusted to HIE.
29(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)	Whether such entity will be pre-registered under DISHA act or whether software used by the entity will have to get license/certificate from recognized agency / HIE to which it transmits?
29(5) Para 3: 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	This clause will create various administrative issues. The insurance company should access data from HIE directly with consent of the patient. What if patient does not give consent to CE but gives consent to insurance company? In that case, CE cannot transmit data to the insurance company or to the HIE.
30(5)and(6) Provided that.. shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.	What happens to the data which has been transmitted to HIE by the CE. Whether it is responsibility of CE to delete the data from HIE or whether CE should forward the request to HIE which will do the needful under advice to CE?
33(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.	What happens if the encryption protocol used by CE is different from one used by HIE or one used by other CE which accesses the data on a later date.
33(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,	Is the consent to be taken at the time of every encounter or one time at the time of registration with CE?.
33(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 heath information exchanges *inter se*.	Between HIE and CE should be added to above list.
34(4) In case where access to digital health data is necessary for the purpose of investigation into cognizable offences, or for	What happens if person who is being investigated for cognizable offense withdraws the consent given to the CE? Also if the HIE provides data to the investigating authority before CE deletes

administration of justice, such access may be granted to an investigating authority only with the order of the competent court;	the data from the HIE?
34(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.	Whether this should remain "access only" is important issue. Patient should be able to add/edit personal health record which will help to facilitate tracking of various parameters such as blood sugar, pulmonary function test, exercise record etc which are important in monitoring chronic diseases. Data generated by CE should be only accessible to patient and data generated by patient should be only accessible to CE.
34(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;	Certain should be replaced with ALL. Will the CE get identity of the patient in emergency based on his thumb impression? This is essential for management of unidentified victim of accident who has to be treated and stabilized by CE as per Supreme Court Ruling. It becomes difficult to continue treatment after initial stabilization, and if the patient is transferred to government institution, usually the patient is lost to follow up. (Charges for treatment given cannot be recovered from anyone.)
34(8) Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner.	Does this mean that at the time of consent the CE should ask the patient to give list of legal heirs to whom access should be given and who are barred expressly? Such consent will have to have a statement as under "In case of my death…", or whether the CE should ask for copy of will/ affidavit?
34(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.	Whether such register should be maintained in electronic format or it is required to be maintained in physical format. ? If HIE can provide electronic register of access of data of any patient by any stakeholder, it will avoid duplication of effort. CE should record data generated from patient and transmit the same to HIE. Ambiguity is likely to be generated if register is maintained by both HIE and CE. As another CE can accesses the data from HIE, it will be better if HIE records the access from CE rather than CE creating another register.
35(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.	Whether this duration of 3 days is from date of breach or from date of getting knowledge of the breach?
36 (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.	How can HIE rectify any data without intimation to the CE which created the data. e.g. information regarding allergy to a drug was not given by patient to the CE. Later he asks the HIE to make correction without knowledge of the CE. This will lead to legal complications and unrest amongst CEs.
37(1)(d) Any person damages, destroys, deletes, affects injuriously by any means or tampers with any digital health data.	What happens if the patient removes the consent with request to delete data stored by CE or transmitted to the HIE?
37(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.	How can it be proved that the breach happened at the HIE level and not at CE level? The breach of data is not likely to be of one patient. It will be of all patients treated by one CE, or transmitted to HIE by all CEs.
38 (1) (c) A breach of digital heath data occurs where a person failed to secure the	What are said standards? They have not been clarified in this act. The Electronic Health Record standards rely heavily on

data as per the standards prescribed by the Act or any rules there under; or	Aadhaar number, which has been mentioned in schedule I. What is current status of Aadhaar Number w.r.t. confidentiality of information? Has Supreme Court approved use of Aadhaar for HIE?
38(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.	This provision will discourage all CEs from digitization of health data. Instead of taking consent for collection of digital health data and transmission to HIE, they will take consent for not to digitize data; or to digitize data but not to transmit it to HIE. If the patient refuses consent, NEHA or any other act cannot force CE to collect and transfer health data. Purpose of this act, IHIP and NEHA will be defeated as no data will be available for public health decisions. At least in first few years of NEHA, such legal provision should be avoided.
40(1) (2) (3) Any Person	Person: should it be entity (whether EDP manager of hospital or Hospital as organization)
43(1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made there under, 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.	What if CE has any complaint about HIE / Owner of the data? There is no provision to grant any remedy whatsoever to the generator of digital health data, who has nothing to gain from such digitization? Why would CEs assist MOH&FW by generating and transmitting digital health data, given the unfavorable circumstances created for CE by virtue of this act?
45(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.	This appeal is after getting the order. What about complaint against HIE/Owner of data?
46(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;	it should be 2 or 3 instead of 3 or 4
46(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.	This appeal is after getting the order. What about complaint against HIE/Owner of data?
Schedule I (xiii) Medical records and history;	Should not be included in personally identifiable information as it is required for public health purpose.
(xvi) Any government number, including Aadhaar :	Without Aadhaar linkage HIE is difficult if not impossible.
New Issue: We should not disallow direct sharing of identifiable data for direct patient care between two hospitals.	Direct sharing of identifiable data should be strictly prohibited. All exchange must be via HIE.
Important consideration: 1. Can data generated by another CE after patient's encounter with first CE be accessed by first CE? This has medico-legal ramifications, hence should be thought carefully. 2. How does government plan to include data generated by AYUSH doctors as there are no standards specified for these specialties. 3. What is the procedure for getting the software licensed by vendors, and getting licensed software by CEs so that software glitches can be minimized and chances of misuse of information are reduced?	

In conclusion, IMA Pune primarily and strongly objects to DISHA Act for following reasons:

1. Implementation of various acts for healthcare has created problems to healthcare providers and facilitated increase in corrupt practices in health departments of government. For example:
    a. Consumer protection act : 90% cases frivolous
    b. PCPNDT act : Harassment, no improvement in sex ratio
    c. Clinical Establishment act : Draconian provisions, Karnataka doctors went on strike
    d. National Medical Commission : IMA had to call for nationwide strike
    e. Registration with Authorities (Qualified nurses : not available, Fire NOC : corrupt practices, Building department /Taxes : irregularities at municipal corporations)
    f. Violence against healthcare professionals: implementation of act is not seen on ground.
    g. CPCB act: Sewage treatment plant for hospitals having more than 10 beds?
    h. **Experience with implementation agencies is not good and harassment is likely.**
2. There is no financial support from government / Ministry of Health and Family Welfare for implementation of health information exchange.
3. Accessibility and Equitability issues: Cost of Healthcare will increase as expenditure on the IT infrastructure and Software will have to be recovered from the patients.
4. Doctors are not techno-savy as far as database management and health information exchange is concerned. They have to rely on staff having knowledge in information technology. Vicarious liability of any misdeed done by hospital staff is likely to bring doctors in trouble.
5. Clinical establishments have no control on personnel in health information exchange who are more likely to leak data to those, who can leverage benefit from analysis of the data.
6. MOH&FW notification dt. 28/10/2014 asks clinical establishments to keep data in electronic format for unlimited period and hard copy for 3 years (10 years in MLC). Why both necessary?
7. Privacy and Confidentiality: Some acts e.g. MTP act do not allow doctors to disclose information to any third party. HIE in such cases even with consent will be construed as criminal offense.
8. Clinical establishments should not be required to provide data to patients, insurance companies, other clinical establishments and Health Information Exchange. CE should give data to patient who may transfer the data to other stakeholders including patient's relatives.
9. Punishment provided in the act is not graded as per severity of crime. 5 year imprisonment and Rs. 5,00,000/= fine are too harsh. There should not be criminal prosecution and erring doctor should be given warnings (three times) and finally closure.
10. Aadhaar Card is not available to each citizen and use of this number has not been authenticated by Supreme Court of India.

Recommendations: Concept of Digital Information Security and HIE are good and essential for having health database of entire population. However population of our country is huge & diverse.

1. The act should be implemented in phased manner, initially only for exchange of information of:
    a. Notifiable Diseases (exemption from punishment for disclosure of information under CRPC, and Offense under IPC if not reported to appropriate authority already exists which should be strictly implemented.) This will remove necessity of consent from the patient.
    b. Pregnancy related information from diagnosis to delivery which will help to improve sex ratio.
2. Ministry of health and family welfare should provide financial assistance for
    a. Training of manpower / skill development
    b. IT infrastructure / tax benefits to hospitals
    c. Internet connectivity and bandwidth utilization
3. Review of utility of digital record systems such as MCTS, HMIS, IDSP etc and policy related statistics of implementation of these programs in various states will help framing strategies for implementation.

Copy to: All MPs in Maharashtra State**,** MP secretariat in Parliament for circulation to all MPs in INDIA.