January 2022

Privacy and Confidentiality of Personal Health Data in Bangladesh

Md Humayun Kabir, D4I[1]

Introduction[2]

Maintaining the privacy and confidentiality of health data is a global issue. With or without knowing it, people share several types of personal data during their interactions with health care service providers and health facilities. As digital systems now record and store this data, issues relating to privacy and confidentiality assume a much greater importance. Health data is sensitive and reveal personal details; it is therefore critical to institute measures to avoid unauthorized access and use of it. This policy brief examines the generation and use of personal health data in Bangladesh and explains why the government should enact appropriate laws and adopt measures for protecting privacy and confidentiality of personal health data within the national digital health infrastructure.

Health Data Digitalization

Measures are needed to safeguard health data collected through digital systems

Digital technologies have penetrated every nook and corner of our world. The health sector is becoming digitized, impacting the operations of health facilities and health care providers. Capturing and storing data electronically offers opportunities for use and reuse of health data, as well as the transmission of data outside the premises. The health domain is now replete with mobile devices (especially in developed countries) that collect and transmit digital data and are used to monitor patient status. This type of data transmission bypasses the traditional health provider's domain and cedes control to the devices' manufacturers. The potential for unregulated data collection and their use or reuse may compromise the security and confidentiality of patient data. Globally, governments encourage development in information and communication technologies (ICT). Privacy and security safeguards must be embedded in all phases of health ICT systems development (Wambugu & Villella, 2018).

Health records digitization in health facility settings began with electronic medical records (EMR). The EMR is a digital version of a patient's treatment history created in a particular facility. The scope of an EMR is limited and is not intended for sharing with others. However, with adoption of relevant standards and protocols, their functionalities could be expanded. A committee in India observed that EMR could provide real-time data access and be used for evaluation in medical care if developed longitudinally (EMR Standards Committee, MOHFW, 2013).

[1] Md. Humayun Kabir, Senior Strategic and Technical Advisor, Data for Impact Project, UNC at Chapel Hill

[2] We are grateful to the following persons for provided valuable input during discussions: Mr. Sukhendu Sekhar Roy, Senior Systems Manager, MIS, DGHS. Mr. Abdullah Al Mamun, Professor, United University. Mr. Ashraf, Vice Chairman, eGeneration and Former Executive Director, Bangladesh Computer Council. Mr. Mohammad Golam Kibria USAID STAR Fellowship Project and Mr. Abdul Hannan Khan, HIS Advisor, DGHS helped with verification of data in tables.

Electronic Health Record (EHR) records a person’s healthcare encounters over his/her lifespan. These records generally contain treatment history, diagnostic reports, and laboratory images. They are accessible through computer networks from different locations. Approved standards for medical vocabulary, clinical content and communication standards ensure interoperability for sharing data within a Health Information Exchange (HIE). The implementation of EHR systems in a facility is a complex undertaking and needs to be implemented with great care, with attention given to context, content, process issues, and the interactions between these. Challenges in handling the complexity of medical data, data entry problems, security, and confidentiality concerns can arise (Boonstra et al., 2014). Digital systems come with risks (i.e., ensuring security and confidentiality of personal health data), but anticipated positive effects on the performance of health system outweigh such risks.

Privacy and Confidentiality

Data privacy is rights-based, and data and system security must protect it

The COVID-19 pandemic that continues to ravage the world has brought privacy issues into the forefront. Countries moved swiftly to repurpose mobile phone records to monitor the spread of the virus, yet at the same time they have struggled to balance privacy and information misuse concerns. Safeguards are required for personal data within a rights-based approach with individual protection (World Bank, 2021).

Health data elements that can identify a patient are considered personal health information (PHI). Health systems, while needing to continue to use PHI for treating patients or other system-related functions, should also ensure privacy, security, and confidentiality. The United States Health Insurance Portability and Accountancy Act (HIPAA), enacted in 1996, has been instrumental in establishing safety criteria around such elements in the health domain. HIPAA defines individually identifiable health information as “Any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearing house; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, including payment for the provision of health care to an individual.” It also includes those having a reasonable basis to believe that the information can identify the individual (USA, 1996). Wrongful disclosure of individually identifiable health information is considered an offense punishable by both financial penalties and jail terms.

IT systems are vulnerable to several types of threats that arise from user behavior, lack of security arrangements, and malicious attempts to break into the system. Data could be breached at different stages whether at rest, during transmission, or at a transfer site. Privacy of health data recognizes people’s rights to control access to their personal health information. Ensuring privacy requires security, protection measures, and tools to safeguard health information and health information systems from unauthorized access or modification of information while maintaining access for authorized users. As such, data security and system security are intertwined. Data security measures are intended for safeguarding data and computer programs from undesired occurrences and exposures. System security covers safeguards associated with hardware, software, personnel, and enterprise-wide institutional policies. Confidentiality has been defined as either a tool to protect privacy or an act limiting disclosure of private matters (Kumar & Wambugu, 2015). Issues of privacy resulted in expansion of EHR into Personal Health Records (PHR).[3] PHR is based upon the recognition of data ownership by the patient.

[3] PHR was proposed in 2006 and defined as an International Organization for Standardization (ISO) standard (ISO/TR 14292).

Personal Data Collection in Bangladesh's Health Sector

Numerous systems in the private and public sectors collect personal health information

The Government of Bangladesh has a Digital Bangladesh vision. This vision includes ensuring delivery of government services to all citizens through the use of technology with the goal of improving the lives of Bangladeshi people. The Ministry of Health and Family Welfare (MOHFW) and organizations under its purview carry this vision forward. The Directorate General of Health Services (DGHS) operates service delivery networks through a combination of primary, secondary, and tertiary hospitals, including specialized hospitals. The Directorate General of Family Planning (DGFP) also operates first-line facilities along with Mother and Childcare Welfare Centers (MCWCs) across the country. The MOHFW takes on the responsibility of primary health care in rural areas, but in urban areas it is vested in local government institutions. The private sector is a major player in the provision of health care both in urban and rural areas. The number of facilities and hospital beds under the private sector are greater than those under the public sector. Therefore, digital health systems across both sectors should be treated similarly for PHI.

The 2018 Bangladesh National ICT Policy calls for connecting all private and NGO providers to high-speed networks and to frame laws, if necessary, to facilitate digital health service delivery. It promotes the creation of portable EHR with appropriate laws. A digital enterprise structure for health in conformity with the National e-governance Architecture is also suggested (তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ, 2018). The implementation status, however, is not known. The MOHFW pursues a sector wide approach and the MIS Operational Plan (OP) of the DGHS is responsible for introducing EHRs, called Shared Health Records (SHR). SHR is intended for generating unique health identity numbers for EHR to connect with medical records. However, concerted efforts are not noticeable. A standards document remains as an incomplete and outdated draft (DGHS, 2012). However, DGHS is utilizing standard open-source hospital management software—like OpenMRS— which have many standards built-in. There is a geo-location registry that could be used to identify facilities, both government and licensed private, but data integrity of that is questionable. The Digital Health Strategy remains unapproved.

A recent D4I review of digital tools in use by the MOHFW demonstrated that different organizations under the MOHFW are using 114 tools (Md. Humayun Kabir & Mohammad Golam Kibria, 2021). Thirty-six of these systems collect personal data and five tools provide authenticated users access to personal data through web-based interfaces (see Table 2, Appendix A). While public sector data reside in country databases, the private sector uses international Data Centers[4] with cross-boundary implications.

Other Countries' Experience with Health Data

Looking to other countries, especially India, as leaders in the field

HIPAA established benchmarks in healthcare information security that spurred many countries to develop their own regulations. Proximity and other similar characteristics, suggest it would be worthwhile to look at the South Asia region, and especially the Indian experience, in terms of setting standards, proposing laws for protection of privacy and confidentiality of health data, as well as creation of appropriate institutions, as explained in Table 1:

[4] There is also concern for security of some data centers under the private sector. However, the government has established a national data center (categorized as Tier 4) capable of meeting government requirement and more.

Table 1. India's Privacy Protection, Digital Healthcare Regulations, and Other Activities

Law/Guidelines	Coverage	Year
The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[5]	This rule, framed under the 2000 Information Technology Act, defines sensitive personal data or information (SPDI), that includes among others, "physiological and mental health conditions, sexual orientation, medical records and history."	2011
Electronic Health Record Standards for India[6]	Pre-defined standards for information capture, storage, retrieval, exchange, and analytics including images, clinical codes, and data	2013, revised in 2016
Digital Information Security in Healthcare Act (DISHA) (Draft circulated in 2018; not yet passed by Parliament[7])	Act aimed at the "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." Digital health data defined as an individual's electronic record of health-related information.	Yet to be enacted
National Digital Health Blueprint[8]	The MOHFW proposed a National Health Stack within the National Digital Heath Blueprint. It details how to establish a comprehensive, nationwide integrated Digital Health ecosystem allowing interoperability of digital health systems at the patient, hospital, and ancillary healthcare provider level. Approval was given by the National Health Authority (NHA), a newly created organization charged with implementing the National Digital Health Mission. This organization is also responsible for India's flagship public health insurance/assurance project, Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB-PMJAY).	2019
National Digital Health Mission[9]	Mission to create a national digital health ecosystem that supports universal health coverage in an efficient, accessible, inclusive, affordable, timely, and safe manner that provides a wide range of data, information, and infrastructure services. Duly leverages open, interoperable, standards based digital systems and ensures security, confidentiality, and privacy of health-related personal information. NHA is responsible for its implementation. It distinguishes between personal and non-personal data. The MOHFW also formulated a Health Data Management Policy as a guidance document across the National Digital Health Ecosystem (NDHE), setting minimum standards for data privacy protection to ensure compliance with relevant and applicable laws, rules, and regulations.	2020
National electronic Health Authority (NeHA)	The NeHA was proposed as a promotional, regulatory, and standards-setting organization. NeHA., if created, would act as the statutory body to promote and adopt eHealth standards and storage and exchange of EHR records.	Proposed

The issue of privacy and confidentiality of PHI has been debated within India and its citizens seek directives from the superior courts. A case in the state of Kerala concerning the sharing of data with third parties and protecting data of COVID-19 positive patients, the Kerala High Court, on April 24, 2020, directed the state government to anonymize the data before sharing it with a third party (in this particular case, a U.S. company).[10] The Court also directed the state government to apprise and receive explicit consent from citizens to maintain confidentiality if data may be accessed by third parties.

[5] https://www.indiacode.nic.in/ViewFileUploaded?path=AC_CEN_45_76_00001_200021_1517807324077/rulesindividualfile/&file=GSR313E_10511(1)_0.pdf

[6] Based on the recommendation of the EMR Standards Committee formed by Ministry of Health and Family Welfare in 2011. Report available here: https://main.mohfw.gov.in/sites/default/files/24539108839988920051EHR%20Standards-v5%20Apr%202013.pdf. Standard v.2 at: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf. Also see: https://www.nrces.in

[7] Available at: https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf

[8] https://main.mohfw.gov.in/sites/default/files/Final%20Report%20-%20Lite%20Version.pdf

[9] https://nha.gov.in/assets/uploads/NDHM_Strategy_Overview.pdf

[10] https://www.mondaq.com/india/operational-impacts-and-strategy/941244/kerala-high-court-issues-guidelines-to-anonymize-data-collected-by-the-state-with-respect-to-covid-19

Findings/Observations

Bangladesh Needs a Specific Law for Personal Health Data Protection

Currently, no specific law exists to protect health data in Bangladesh. An in-progress Digital Health Strategy draft includes the following in its objectives: "the guarantee of patient information rights, integrity, privacy, security, confidentiality, and anonymity in line with emerging public health access needs. Privacy and security of personal health information stored in shared electronic health records and personal health records at entity level will be ensured both in storage and transmission" (MOHFW, Government of Bangladesh, 2021).

Nor is there a law for the protection of personal data or privacy. In countries where health data laws are absent, ICT-related laws provide some guidance. The Bangladesh Digital Security Act (DSA 2018) is intended to ensure cyber security. The DSA 2018 makes provisions for punishment for collecting, using identity information without permission[11] (Government of Bangladesh, 2019). A draft of a new privacy law was shared on a government website for a limited time seeking public opinion. It is not yet known whether it will cover health data and if so, how.

Sharing health data relies upon the consent of the owner (individual) and the controllers or organizations that have legal responsibilities for ensuring its privacy. All stakeholders such as service providers, body corporates, and other users need to ensure the privacy of data with the express provision of consent and anonymization if/when case data is shared with third parties (Farn et al., 2007).

Many countries have created or plan to create separate entities for managing eHealth infrastructure and EHR. The existing organizations under the MOHFW lack core competencies in managing digital health initiatives. Creating a separate organization under the MOHFW for managing eHealth infrastructure is a critical next step.

Recommendations

The following recommendations are based on the information presented herein:

a) Bangladesh needs dedicated data protection laws for health, highlighting privacy, and confidentiality of personal health data.

b) The MOHFW should take a holistic approach and address health data through standards setting, interoperability frameworks, and a health information exchange covering public and private sector facilities, providers, and other stakeholders.

c) Bangladesh should create a competent organization backed by appropriate legislation to manage its eHealth infrastructure.

[11] The law defines "Identity Information" as "any external, biological or physical information or any other information which singly or jointly can identify a person or a system, his/her name, address, date of birth, mother's name, father's name, signature, national identity, birth and death registration number, finger print, passport number, bank account number, driver's license, E-TIN number, electronic or digital signature, username, credit or debit card number, voice print, retina image, iris image, DNA profile, security-related questions or any other identification which due to the excellence of technology is easily available."

References

Boonstra, A., Versluis, A., & Vos, J. F. (2014). Implementing electronic health records in hospitals: A systematic literature review. *BMC Health Services Research*, *14*(1), 370.

DGHS. (2012). Health Informatics Standards and Data Structure for Bangladesh. http://dghs.gov.bd/images/docs/eHealth/Standards_and_interoperability_document_final_5.01.14.pdf

EMR Standards Committee, MOHFW. (2013). Recommendations On Electronic Medical Records Standards in India. https://main.mohfw.gov.in/sites/default/files/24539108839988920051EHR%20Standards-v5%20Apr%202013.pdf

Farn, K.-J., Hwang, J.-M., & Lin, S.-K. (2007). Study on Applying ISO/DIS 27799 to Healthcare Industry's ISMS. Proceedings of the 6th Conference on WSEAS International Conference on Applied Computer Science. 4(8), 15.

Government of Bangladesh. (2019). The Authentic English Text of the Digital Security Act, 2018.pdf. Legislative and Parliamentary Affairs Division. https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/law/e883dda8_4ee4_4f4f_89f2_3d50685ebd3f/The%20Authentic%20English%20Text%20of%20the%20DIGITAL%20SECURITY%20ACT,%202018.pdf

Kumar, M., & Wambugu, S. (2015). A Primer on the Privacy, Security, and Confidentiality of Electronic Health Records (p. 13). MEASURE Evaluation. https://www.measureevaluation.org/resources/publications/sr-15-128-en/at_download/document

Md. Humayun Kabir & Mohammad Golam Kibria. (2021). HIS Mapping: An Inventory of Digital Tools in Use by the Ministry of Health and Family Welfare in Bangladesh [Policy Brief]. Data for Impact (D4I) Project, UNC at Chapel Hill. https://www.data4impactproject.org/publications/his-mapping-an-inventory-of-digital-tools-in-use-by-the-ministry-of-health-and-family-welfare-in-bangladesh/

MOHFW, Government of Bangladesh. (2021). Digital Health Strategy (Draft).

Shahzeb Mahmood. (September 13, 2021). Bangladesh's new data protection act: Brittle shield or blunt sword? *The Daily Star*. https://www.thedailystar.net/views/in-focus/news/bangladeshs-new-data-protection-act-brittle-shield-or-blunt-sword-2174371

USA. (1996). Health Insurance Portability and Accountability Act. https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

Wambugu, S., & Villella, C. (2018). *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and Opportunities in Data Quality, Privacy, and Security* (p. 20).

World Bank. (2021). World Development Report 2021: Data for better lives. https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ. (2018). *জাতীয় তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা ২০১৮* (National ICT Policy 2018). https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/704b7e34_bef2_422d_9645_8ebf90e6eca7/National%20ICT%20Policy%202018.pdf

ফখরুল ইসলাম & নুরুল আমিন. (October 2, 2021). *ই-কমার্সের নামে প্রতারণা: কেউ এখন দায় নিচ্ছে না.* https://www.prothomalo.com/business/%E0%A6%95%E0%A7%87%E0%A6%89-%E0%A6%8F%E0%A6%96%E0%A6%A8-%E0%A6%A6%E0%A6%BE%E0%A7%9F-%E0%A6%A8%E0%A6%BF%E0%A6%9A%E0%A7%8D%E0%A6%9B%E0%A7%87-%E0%A6%A8%E0%A6%BE

Appendix A

Table 2. MOHFW HIS tools generating or having access to personal health data

Sl	Tool/System	Organizations
1	OpenSRP - PRIMA (integrated with SHR)	Community Clinics
2	MHV app (CHCP community tracker)	Community Clinics
3	DHIS2 - Cervical and breast cancer surveillance system	DGHS, DGFP, NGOs, BSMMU
4	Adverse Drug Reaction Reporting – COVID-19 AEFI reporting system	Directorate General of Drug Administration
5	eMIS - FWA eRegister	Directorate General of Family Planning
6	eMIS - Facility Systems eRegister (first-line facilities provider)	Directorate General of Family Planning
7	eMIS - Health and Family Planning ID printing system	Directorate General of Family Planning
8	DHIS2 - COVID19 surveillance system	DGHS and private sector organizations
9	DHIS2 - Mortality (causes of death) reporting and notification	DGHS, All Hospitals (Private and Public)
10	DHIS2 - CHCP Community tracker	Directorate General of Health Services
11	DHIS2 - AEFI and VPD surveillance system	Directorate General of Health Services
12	DHIS2 - Maternal, Child and general patient reporting system	Directorate General of Health Services
13	DHIS2 - Maternal and Perinatal Death Screening and Review	Directorate General of Health Services
14	Shared Health Record (SHR)	Directorate General of Health Services
15	DHIS2 - NASP reporting system including PLHIV & PMTCT	Directorate General of Health Services
16	OpenMRS+	Directorate General of Health Services
17	Telemedicine System	Directorate General of Health Services
18	eMIS - HA eRegister	Directorate General of Health Services
19	eMIS - AHI eRegister	Directorate General of Health Services
20	eMIS - HI eRegister	Directorate General of Health Services
21	DHIS2-Immunization registry (e-Tracker)	Directorate General of Health Services
22	eTB Manager	Directorate General of Health Services
23	GxAlert	Directorate General of Health Services
24	Shasthyo Batain 16263: Health Call Center	Directorate General of Health Services
25	NCD-eMIS	Directorate General of Health Services
26	COVID-19BD	Directorate General of Health Services
27	National public COVID-19 portal of DGHS	Directorate General of Health Services
28	DHIS2 - HMIS System for Forcibly Displace Myanmar Nationals (FDMN) (both aggregated reporting and EPI tracker)	Directorate General of Health Services
29	DHIS2 - NCD trackers	Directorate General of Health Services

30	DHIS2 - Hospital in-patient HMIS system	Directorate General of Health Services
31	SSKMS	Health Economics Unit, MOHFW
32	IEDCR AMR surveillance system	IEDCR
33	Surokkha app	MOHFW and ICT Division
34	COVID19 test certificate validation and verification	Ports, immigration, airlines, and public
35	Self-service COVID19 test result reporting system	Public use though OTP
36	eMIS - FPI eSupervision System (web-based)	Directorate General of Family Planning
37	eMIS - UFPO eManagement System (web-based)	Directorate General of Family Planning
38	eMIS - Facility dashboard (web-based)	Directorate General of Family Planning
39	Sukhi Poribar (16767) (web-based)	Directorate General of Family Planning
40	eMIS - community Dashboard (web-based)	Directorate General of Family Planning
41	eMIS - UHFPO eManagement System (web-based)	Directorate General of Health Services

Note: Some web-based tools have very restricted access to individual records through web-based tools.

For more information

D4I supports countries to realize the power of data as actionable evidence that can improve programs, policies, and—ultimately—health outcomes. We strengthen the technical and organizational capacity of local partners to collect, analyze, and use data to support their move to self-reliance. For more information, visit https://www.data4impactproject.org/

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of the Data for Impact (D4I) associate award 7200AA18LA00008, which is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill, in partnership with Palladium International, LLC; ICF Macro, Inc.; John Snow, Inc.; and Tulane University. The views expressed in this publication do not necessarily reflect the views of USAID or the United States government. WP-21-250_D4I