

Summary of eDiscussion

Name of participant	<i>Byoung-il Oh</i>
Designation	
Organization	<i>Korean Progressive Network Jinbonet</i>
Email	<i>antiropy@gmail.com</i>

In South Korea, medical data, generated in the hospital in general, has been protected by MEDICAL SERVICE ACT, which is not an act for the purpose of data protection but includes some provisions for data protection and data security, such as article 18(3) and 23(3) for data security, article 19 for prohibition of leaks of medical data.

Remote medical treatment, which is articulated in Article 34, is allowed under very limited conditions.

MEDICAL SERVICE ACT

[Enforcement Date 19. Mar, 2010.] [Act No.9932, 18. Jan, 2010., Other Laws and Regulations Amended]

SECTION 2 Rights and Duties

Article 19 (Prohibition of Disclosure of Confidential Information)

Except otherwise as provided by this Act or other Acts and subordinate statutes, a medical person shall not divulge or disclose any person's confidential information he/she becomes aware of in the course of performing medical treatment, assistance in childbirth, or nursing.

Article 21 (Inspection of Records, etc.)

(1) No medical person or any person working for a medical institution may release the details of a patient's records or make them accessible, such as providing a copy thereof, to any person, other than the patient. <Amended by Act No. 9386, Jan. 30, 2009>

(2) Notwithstanding paragraph (1), each medical person or any person working for a medical institution shall release the details of a patient's records or make them accessible, such as providing a copy thereof, in any of the following cases: Provided, That where a medical doctor, dentist or oriental medical doctor deems it necessary to treat the patient, this shall not apply: <Amended by Act No. 9386, Jan. 30, 2009; Act No. 9932, Jan. 18, 2010>

1. Where a spouse, lineal ascendant or descendant of a patient, or a lineal ascendant of the spouse makes a request meeting the requirements prescribed by Ordinance of the Ministry of Health and Welfare, such as accompanying the consent of the patient in question, a certificate proving kinship and any other documents;

Article 23 (Electronic Medical Records)

(1) A medical person and the founder of each medical institution may, notwithstanding Article 22, prepare and keep medical records, etc. in the form of an electronic document with a digital signature therein under the Digital Signature Act (hereinafter referred to as "electronic medical records").

(2) A medical person and the founder of each medical institution shall have facilities and equipment required for managing, controlling and preserving electronic medical records safely in compliance with

Ordinance of the Ministry of Health and Welfare. <Amended by Act No. 8852, Feb. 29, 2008; Act No. 9932, Jan. 18, 2010>

(3) No one may leak, alter or destroy any personal information stated in an electronic medical record without any justifiable reason.

Article 34 (Remote Medical Treatment)

(1) Medical persons (limited only to medical doctors, dentists or oriental medical doctors who engage in medical service) may, notwithstanding Article 33 (1), give remote medical treatment (hereinafter referred to as "remote medical treatment") to furnish medical knowledge or technology to a medical person in a remote area by using information communication technology, such as computers or visual communication systems.

(2) A person who intends to give or take remote medical treatment shall have the facilities and equipment prescribed by Ordinance of the Ministry of Health and Welfare. <Amended by Act No. 8852, Feb. 29, 2008; Act No. 9932, Jan. 18, 2010>

(3) A person who gives remote medical treatment (hereinafter referred to as "remote doctor") shall have the same responsibility as when he/she gives direct medical treatment to a patient.

(4) If a medical person, who has performed medical practice following a remote doctor's remote medical treatment, is a medical doctor, dentist or an oriental medical doctor (hereinafter referred to as "local doctor"), and if there is no obvious ground to believe that the remote doctor is negligent in performing his/her medical practice, the local doctor shall be responsible for a patient, notwithstanding paragraph (3).

Summary of eDiscussion

Name of participant	<i>Janice L. Krieger</i>
Designation	<i>Director</i>
Organization	<i>STEM Translational Communication Center College of Journalism and Communications University of Florida, USA</i>
Email	

In USA electronic health data policy called HIPAA (Health Insurance Portability and Accountability Act) and is quite extensive.

Summary of HIPPA rules:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security

Rules: Protect individually-identifiable health information and grant rights grant to individuals concerning the privacy and security of their data.

The HIPAA Privacy Rule: Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. (Department of Health and Human Services)

The HIPAA Security Rule: Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. (Department of Health and Human Services)

The Office for Civil Rights of the U.S. Department of Health and Human Services is responsible for enforcing the **HIPAA Privacy Rule and the HIPAA Security Rule**, as well as the confidentiality provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA) or Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

Summary of eDiscussion

Name of participant	<i>Lisa Garcia</i>
Designation	
Organization	Foundation for Media Alternatives (FMA), <i>Philippines</i>
Email	

Philippines has the Data Privacy Act (RA 10173), which is the prevailing data protection law for both government and the private sector in the Philippines, as well as its implementing rules.

Another is Joint Administrative Orders (JAO) from three government agencies on the Philippine Health Information Exchange (PHIE). The PHIE allows participating health care providers to share health information and harmonizes health data from various EMR and hospital information systems. JAO 2016-0001 contains general guidelines for PHIE implementation, whereas JAO 2016-0002 contains the privacy guidelines.

Guided by the PeHSP for UHC/KP, one of the identified critical eHealth projects is the Philippine Health Information Exchange (PHIE). The PHIE is a platform for secure electronic access and efficient exchange of health data and/or information among health facilities, health care providers, health information organizations, and government agencies in accordance with set national standards in the interest of public health.

SUMMARY OF POLICY RELATED TO ELECTRONIC HEALTH DATA PRIVACY IN-

Joint Administrative Orders JAO 2016-0001 MENTIONED --

2.2. Patients—

(a) Patients shall be required to accomplish the Patient's Informed Consent regarding individual participation in the PHIE. If a patient agrees to participate in the PHIE, **all sensitive** personal information shall be made available for query to all participating PHCPs through the PHIE.

b. For request for amendment of sensitive personal information, patients shall be required to submit the accomplished PHIE Request for Amendment form to the PHIE Management Group for their endorsement to the concerned PHCP that provided the sensitive personal Information for appropriate action.

3. Access Management

4. Sharing and Exchange of Health Data/Information

The standard protocol for sharing and exchange of health data information for PHIE shall be in accordance with the operational guidelines and requirements for sharing and exchange of health information contained in the approved PHIE Manual of Operations, taking into utmost consideration the relevant and applicable Philippine laws, particularly to the following provisions of Republic Act 10173:

5. Appropriate Use and Disclosure

5.1. Sensitive personal information must be used for treatment and care coordination purposes only or to the extent necessary and permitted by applicable Philippine laws and regulations and policies of the PHIE.