

## **CONSOLIDATED WORKSHOP OUTPUT FROM ANGELES, PAMPANGA**

**Date: Nov. 26-27, 2015**

### **Station 1: Collection and Processing of Health Information**

#### *A. Processing of Health Information (Collection/ Identification of Patient/ Data to be collected/ information to be shared)*

1. Security Officer shall be responsible in orienting the patients regarding the PHIE implementation and validation of the patient's data/information. If no designated position for security officer, kindly assign a full-time security officer.
2. Include chief privacy officer as a requirement in the licensing of hospitals.
3. Privacy Officer's duties:
  - a. Ascertain the authority of persons entering or encoding the data.
  - b. Ensure no unauthorized editing of data happens.
  - c. Document the entire process of editing data:
    - i. Request for editing
    - ii. Reason for editing
    - iii. Who did the editing
    - iv. the process followed in editing
    - v. Closing the process of editing.
4. All diagnostic records is intended for viewing only to maintain the confidentiality and so not to violate the hospital procedures on reproducing certified true copy of records.
5. Destruction of data (whether illegitimate or not) is not suggested because of the following purposes:
  - a. Future reference for possible illegitimate data
  - b. Data audit trail
6. GCP guidelines on changing data on information should be complied:
  - a. Original entry should be visible
  - b. Change must be dated and countersigned.
  - c. Reasons for the changes must be entered or specified.
7. There must be specific guidelines for proper encoding, recording, and storage of data.
8. Time of encoding/ processing should be specified. Suggestion after discharge.
9. Provide a list of approved options in activating personal health information upon entry/visit to a health facility.
10. Best practices on Health Information Exchange must be considered.
11. For patients who do not want to upload their data, an option to de-identify him may be clicked. For the other facility to view it, an authorization form will be filled-out.

#### *B. De-Identification*

1. De-identification at the PHCP level for immediate statistical reference.

#### *C. Creation of Shared Health Record*

1. Redefine the concept of Sharing (e.g. the fact that the consent is signed, it implies that you are allowing your records to be shared)

#### *D. Consent*

1. Include in the patient's consent that data shall be used in research.
2. Triage personnel should/must be oriented regarding PHIE and Consent form for Data collection.
3. Patient's consent can be stored electronically.
4. Specified time of validity of patient's consent must be specified.
5. For public education: DOH and PhilHealth shall make an abstract of truth/poster/AVP/comics or message regarding the PHIE that patients will clearly and comprehensively understand.
6. An opt-out clause shall be provided/included in the ICF.
7. *For elevation to PEG: When is the best time to obtain the consent? Upon admission or discharge?*

#### *E. Recommendation:*

1. To allow healthcare providers to comply with the medical records requirements electronically (i.e. avoid the cost of storing paper records for 5 years OPD, 10-15 years for in-patients, and forever for medico-legal cases). This will also encourage providers to connect to PHIE.

### **Station 2: Access of Health Information**

#### *A. Authentication to Access*

1. Delegate 2 system administrators that will serve as a system/data auditor.
2. PHIE policies on access of user:
  - a. Don't give UID and PWD
  - b. Don't let your secretary access the data for you.
3. Add more specific guidelines for Joint AO VII, item 1.C. Specify what data is to be shown.

#### *B. Access to Shared Health Record*

1. Assign user roles per staff to manage access of the staff per station.
2. Who will have the right to access the patient data if the patient is not capable to access it, or if the child's parents got separated?
3. What to be added for 2<sup>nd</sup>/3<sup>rd</sup> Health provider (read-only):
  - a. Adverse effect of medication provided
  - b. Treatment outcome. Final diagnosis should be included whether clinical or confirmed.
  - c. Access/information about laboratory diagnostic procedure results.
4. Access by patient to his own information should be allowed based on patient's preference on which for portal provider to use basing on user experience. Reliabilities and other tasks vary and patients have the preference.

#### *C. Recommendation*

1. Double check the patient charts if complete or incomplete before saving the information to the MIS.

### **Station 3: Uses and Disclosure of Health Information**

#### *A. Disclosure to a third party*

1. Protocols for requesting and accessing aggregate and de-identified information for research both public and private should be clearly identified.
2. Situation: HMO requesting for health records of the patient:
  - a. There should be a clear agreement or a contract should be made that will stipulate consent of patient enrolled in HMOs.
3. Disclosure of medical records to medical students:
  - a. Guidelines for retrieval of information for purposes of PRC requirement for compliance of application abroad should be made.
4. In case of a deceased patient separated with his/her partner but not legally separated, and the partner is requesting for the patient's health record for purposes of claims, what is the rule for disclosure?
5. Medical representatives should review their contract.

#### *B. Confidentiality of Privileged Information*

1. For unconscious patient: spouse, relative or the doctor can ask for the decision of the family. In case of an unconscious patient with no relative, the doctor can decide in behalf of the patient.

#### *C. Responsibility of PHCP*

1. Issue: Facilities that do not participate in PHIE, in-case of de-identified data, PHIC will hold the benefits or the capitation:
  - a. A workflow should be made. A need for a notification protocol. Suggest making a flow chart. (Suggested to use the present epidemiologic surveillance framework)
  - b. Health facility shall immediately notify the RESU (using the present framework)
  - c. DOH notifies the EMR, EMR to the facility.
  - d. EMR suggested to having a code which gives them the signal to release the information.

#### *D. Information to be disclosed*

1. Clarification on the de-identification of health information. Only de-identified health information shall be stored in the PHIE Data Warehouse. In what level does the de-identification take place?
  - a. Atty. Ivy suggested that the de-identification should take place in the PHCP
2. Protocols for disaster response should be made.
3. Additional form (withdrawal form) for patients who want to opt-out with guidelines/information relayed with the patient.

#### *E. Recommendations:*

1. In case of minor patients, notify them when they come of legal age.

2. Creation of IRB on ethical standards to all government and private health sectors to monitor disclosure of health information.
3. Accreditation of research facilities by DOH.
4. Suggest to PRC to require other certification instead of requiring nursing students applying for NLE to submit the list of cases that these students handled.

#### **Station 4: Data Security**

##### *A. Organizational Security Measures*

1. Assign a Privacy Officer, PHIE Compliance Officer, Management Information Systems Officer (MISO)
2. Duties and responsibilities of the Privacy Officer, PHIE Compliance Officer, MISO:
  - a. Monitor, account and register devices used in facility.
  - b. Perform system or quality data check, compliance on the reporting form and safekeeping of backup data.
  - c. Delegate data collection to staff but should ensure that the data collected are correct. The sole responsibility of encoding is on the appointed individual/ unit.
3. Qualifications of a Privacy Officer, PHIE Compliance Officer, MISO:
  - a. A graduate of Masters of Science in Health Informatics.
  - b. With IT, medical or clinical background.
  - c. With training certifications on the security aspect of PHIE. Note: DOH and PhilHealth shall set the minimum standards based on the body of knowledge for data security, which shall be the bases for hiring of a Privacy Officer, PHIE Compliance Officer, and Management Information Systems Officer.
4. Health facility staff-related policies:
  - a. Employment contract should contain provisions regarding data privacy and security.
  - b. Character or personality check of the employee who has direct contact/access to the information system shall be done by the health facility.
  - c. Capacity Building:
    - i. Health facility staff should have regular orientation on policies relating to privacy and security.
    - ii. Training modules on basic security measures shall be created (e.g. training kit using bogus data and demo training site or facility)
    - iii. Authorized personnel handling data shall undergo certification course and be certified by system vendor and both DOH and PhilHealth.

##### *B. Physical Security Measures*

1. Conduct pre-deployment site assessment.
2. The minimum server configuration (hardware) should be specified.
3. The computer to be used must be fixed in one place and not portable.
4. In the event that the machine is lost or stolen, deactivate account until retrieved or reported. However, it is best to reset credentials.

5. Provide multiple back-up mechanics/destination (local machine, external storage, cloud). Back-up should be every day, cloud and offsite.
6. Bringing of smart phones, laptops, tablets and other electronic gadget alike should be prohibited inside the medical records area.

#### *C. Technical Security Measures*

1. Data back-up shall be encrypted or password protected.
2. Provide detailed and specific protocols on encryption methods (e.g. encryption of data at rest)
3. Maintain an activity history log.
4. The PHIE group should provide help desk and perform monitoring of database and network by DB and network administrator.

#### *D. Policies*

1. Governance-related policies:
  - a. include compliance to required PHIE security measures as item in the checklist for PhilHealth Accreditation of the hospital or renewal of license to operate.
  - b. Perform random visits and monitoring of DOH on the implementation of the PHIE program for check and balance purposes
  - c. Identify the diagnosis that needs to be reported and specify exclusions.
2. Patient-related policies:
  - a. There should be a waiver from liability in the event of hacking from the patient.
  - b. There should be participation in reporting policy violations (e.g. hotline)
  - c. Provide information, education and communication (IEC) materials on data privacy and security to patient.