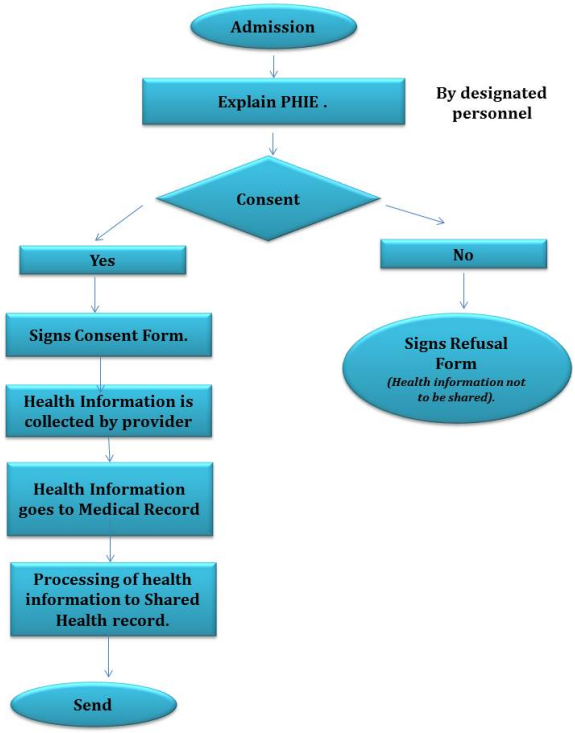
Title of Activity:	Health Data Privacy and Security Workshop Series 3: Mindanao
Date:	October 22-23, 2015
Venue:	The Royal Mandaya Hotel
Topic:	Guidelines for Collecting and Processing of Health Information

Area: Guidelines for Collecting and Processing of Health Information

Flow Chart for Signing of Informed Consent



- We need to present the template of the Consent Form with specific Checklist. Specific checklist must be grouped accordingly (e.g. Personal Data).
- UDRS should be reconciled with this consent form.
- Refusal form for patients who does not want to share his/ her information.
- Agreement and consent must have a local translation.
- Designated person to explain the agreement must not necessarily be the doctor.
- Provision of space in the patient admission form for the signature of the significant others if patient was unable to sign; space for witness to sign.
- Renaming of patient admission form to “Consent for Participation to PHIE”.
- DeFINITION/ Identification of data to be collected as mandatory for submisison to PHIE.
- Simplify the admission form consent.
- Seperate the consent for admission and consent for participation in PHIE.
- Consent for sharing of health information shall be taken upon discharge.
- Printed patient name shall be indicated below the patient admission form.

Area: Access to Health Information

- Add "relationship to patient", "date and time in consents", contact number. The patient should be alive during the time of consent
- For each purpose, meron dapat inclusion and exclusion criteria
- Create a consent form which consist of the part/s of the patient's health records to be retrieved/released. Prior to the release of patients health records. Secure first the consent of the patient to release such , so with the attending physician as a gesture of courtesy.
- In the event that the patient is on coma, a special power of attorney shall be excecutred to establish relationship of next of kin to patient
- A protocol must be defined on how to identify the person
- Different printouts per use, per user.
- Only specific information approved by the patient can be accessed or viewed.
- Only attending physician should have access to the patients who have allowed their information to be viewed.
- 24/7 operations a.k.a call center hotline center/ tech center to allow necessary access infor when required at any time
- Patients may be provided access to their record in PHIE where their doctors are not enrolled yet in PHIE
- Specific clause in the consent that the patient can opt to discontinue to use PHIE.
- Access to information by someone should
- Persons authorized to give consent other than the next of kin: 1. Common partner co-habiting for at least on year, 2. Person with special power of attorney
- Significant others can sign consent in times of emergency situations with witnessess however sharing of information for PHIE is not applicable
- You can give consent on information during admission even if you are not related to patien. But giving consent to share information is a different thing.
- Additional information to be accessed: 1. Medications taken, 2. Laboratories/diagnostic procedure done
- Auto close interface if not accessed for minutes and for accidental viewing of other users

Area: Use and Disclosure of Health Information

- Define what information will be disclosed
- The following data/information that can be disclosed after discharged from the hospital 1. Clinical abstract, 2. Laboratory result, 3. Doctor's order, 4. Discharge summary
- PNP Subpoena Duces Tecum should be honored and compllied with, if signed by the head of the agency
- For authorization: authorization letter and 2 valid ID's
- SPA(special power of attorney) in cases where the person is requesting for info is incapacitated
- A thumbmark should be considered and witnessed by a person of legal age
- Assent for minor patients shall be developed
- Process on how to disclose medico-legal case

Area: Data Security

POLICY:

- Each facility should have its respective policy regarding role-based access control.
- Each health facility that uses health information system should ensure that users of the system are authorized and are provided with access such as username and password.
- Training on IT security policies should be part of the regular trainings of staff.

- Data privacy-related clause should be part of the contract of third party providers. Emphasis should be placed on the ownership of data.
- Provision of data like patient records shall be consistent with the guidelines of hospital health information management manual issued by the Department of Health.

PEOPLE:

- Based on company policies on user account and responsibilities for hospital information system
- A privacy officer should be assigned to regularly audit the quality and integrity of patient record.
- The medical record officer has the authority to audit the patient record from time to time in order to determine the integrity of the patient record.

ACCESS CONTROLS:

- The level of access may vary, but the user credentials assigned to a single individual should be the same.
- The head of the section or unit like medical director or chief nurse shall approve the creation of user credentials for personnel that shall access the hospital information system.
- Best practice for changing of password shall be three to six months.

NOTIFICATION OF BREACHES:

- There should be an escalation process regarding incidents of breach of information/ data
- Recommended definition: Information breach is the unauthorized disclosure of information.
- Information breach can be in the context of patient and institution.
- Sample breach can include:
  Capturing and posting of an image of a person despite being not identified, e.g. part of a body
  Capturing and posting of an image of equipment, specimen, etc.
- Medical students shall not be allowed to access patient's medical record particularly patient history for case study purposes. The students shall produce the information regarding patient's health history by themselves.