Workshop Output
Health Data Privacy Workshop: Visayas Leg
Bacolod City

Station 1: Collection and Processing of Health Information - Ms. Aida Cuadra

A. Consent
    1. A uniform / standard informed consent form shall be developed / provided for health facilities engaged with PHIE. The form shall include a list of information that could be shared and purpose. (Limitation of the information to be shared)
    2. A designated person / staff shall be assigned to obtain the informed consent upon registration / admission.
    3. A limitation in the length of time a patient's information can be shared shall be set.
    4. An opt out clause shall be provided / included in the Informed Consent form.

B. Point of Collection/ Identification of Patient/ Data to be Collected/ Information to be Shared
    1. Collection of information starts at the time of registration in the health facility.
    2. Initial collection is done at the Admitting / Registration section. Subsequent information shall be provided at the different levels of care. Family information / socio – economic profile shall be collected by the Medical Social Worker.
    3. Data collection & processing shall be done by a permanent employee of the health facility. Said employee shall sign a non-disclosure agreement that shall take effect even after separation from service.
    4. As part of ensuring privacy / confidentiality of information, non – disclosure clause shall be included in the Contract of Affiliation of schools.
    5. All information collected at the different level of cares shall be integrated into common file.

C. Filling / Storage
    1. An electronic achieving system shall be developed for the storage of electronic data.
    2. An inactive file / directory shall be created. Included in this file will be the records of expired / deceased patients. Access to these files shall be limited for research purposes only.

Station 2: Access of Health Information - Mr. Rey Verdolaga

1. Standard consent form for all hospitals
2. Information drive on the consents . The DOH such enforce this for the public, private facilities and other HCs.
3. Accessing PHIE - Pin + Security Questions. Official recipients only. Clearly define access rights of encoders/editors of data. username and password expire. audit trail in place & authorize person (open, data entry, print, view, revision, removal, approval). Updating of user access should be done regularly.
4. Access to second health care provider – read only (cannot be printed), if to assist in the management of the present illness
5. Info to be accessed – hx of past illness, family hx of illness, allergies
6. If electronic information system will be used to access information of patient it must be, same language portal to use, user friendly, real time batch period with terminals identified locations
7. Develop a monitoring and evaluation mechanisms.

Station 3: Uses and Disclosure of Health Information – Atty. Ivy Patdu

A. Based on Section 14 of Privacy Guidelines:
    1. Hospitals shall continue keeping patient's health records pursuant to own hospital policy.

2. The PHCP should transmit information from patient's records to the PHIE as a shared health record:
    a. If patient consents, the patient's Shared Health Record may be processed in PHIE without the need of de-identification. This Shared Health Record shall be available for treatment coordination purposes only.
    b. If patient does not consent to participate in PHIE, the patient health information shall be de-identified, containing information necessary for generation of health statistics.
3. For unconscious patient and minor patient, consent shall be given by the following: parents, spouse if married, descendant, ascendant, and guardian; however, it can still be revoked by patient.
4. Use of health information shall include the following purposes:
    - For planning for quality services
    - DOH reporting intervention and diseases prevention
    - Continuing care to patients

B. Based on Section 15 of Privacy Guidelines:
1. DOH may order the use and disclosure of health information
   For identification of a highly contagious diseases and other emergency or disaster situations.
2. The Health facility is in position to identify and recognize serious health and safety threat to the public

   The serious health and safety threat to the public shall include the following:
    - Meningitis, food poisoning (mass)
    - Breakthrough of epidemic contagious disease
    - Biological/chemical warfare
    - Anthrax
    - Notifiable diseases, emerging and re-emerging diseases
    - Ebola

C. Based on Section 16 of Privacy Guidelines:
1. As a general rule, before a disclosure is made to any other government agency, there must be a court order. It is only in cases of emergency, such as that provided in Sec.15, where disclosure can be done without court order. This would be situations where time is of the essence.
2. The situations contemplated are:
    - For PNP Subpoena , obtain consent of patient before death; otherwise consent obtained from next of kin
    - For medical/financial assistance requesting abstracts or similar documents authorization from patient is required.
3. For authorization, the authorizing entity shall provide any of the following for identification: biometrics, specimen signature, e-signature
4. The hospital shall develop a policy for the release of information which includes requirements for identification and authorization

D. Based on Section 17 of Privacy Guidelines:
1. Both patient and physician must provide consent for use and disclosure for privilege communication, otherwise information shall not be released.
2. Privilege communications under the rules of court covers the communication between a physician and patient regarding any advice or treatment given by him or any information which he may have acquired in attending to the patient in professional capacity and which information would blacken the reputation of the patient;

E. Based on Section 18 of Privacy Guidelines:
   1. Participating health care providers should have policy in place.
   2. Hospital will be the custodian of records and has the power to limit access regarding the data to be disclosed.
   3. Use of health information shall only be to the extent of consent given by patient.
   4. Consent of the patient must be obtained on the following:
      a. For research and educational purposes, including use of photographs
      b. Patient information as requirement in taking specialty Board examinations
   5. The consent of the patient may be included in the contract of admission or upon discharge depending on the capacity of patient to consent. It shall include a provision that patient's identify shall be protected.

F. Based on Section 19 of Privacy Guidelines:
   1. As a custodian of Health Information, The PHCP has the authority to disclose information upon patient request for his legitimate personal use
      - Release of insurance/HMO required medical record
      - For patients who are US war veterans, they should come with a signed consent to release medical records.
   2. Unless there is a valid court order, patient records shall not be released or disclosed. Without a court order, release of information shall be pursuant to hospital policy.

G. Based on Section 19 of Privacy Guidelines:
   Legitimate purpose shall include:
      - Requirements and reporting of communicable and notifiable diseases
      - Reporting of serious and less serious physical injury
      - Reporting of a maltreated or abused child to proper authorities.
      - Mandatory reporting required by licensing and accreditation bodies e.g. DOH, PhilHealth, etc.

Station 4: Data Security - Mr. Kit Sumabat

A. Administrative Security
   1. Forma an information security committee where other stakeholders are represented -- medical records, medical director, nursing, front liners, finance, etc.
   2. Medical records officer has the access to patient's data. IT comes in only when assistance on system use, e.g. troubleshooting, happens.
   3. Policy in place on how data transfer shall be facilitated shall be included in the IRR.
   4. Budget allocation where facilities shall be directed to allot funding for the implementation of data security safeguards shall also be included in the IRR
   5. Training-related guidelines shall be incorporated.
   6. Full time employees shall take charge of implementing the data security safeguards.
   7. Put down policy on paper. Hospitals shall have security policies written on paper.
   8. Information security is not included in the ISO of some hospitals.
   9. Password in Hospital Information System (HIS) shall be changed every 3 months.
   10. System access request form should be approved by the head of the facility.
   11. Data inconsistencies (final output) are one of the challenges being experienced in HIS.
   12. User rights, accounts are being removed when the employee has resigned, retired or separated from service.
   13. Security features are being incorporated in the system requirements.

14. Information security officer shall focus on health information rather than IT side.
15. IT should be more of the system functionality. Control of data should be in the hands of the data custodian.
16. User account responsibility shall be taken care of the user account owner.
17. QA group handles information security.
18. HR policies incorporate sanctions for information security violations.
19. Limiting of uploading of information other than the intended purpose.
20. Some hospitals are still in the process of creating a policy for BYOD.
21. Monitoring of the social media accounts of nurses for privacy breaches. No monitoring activity yet for doctors.
22. Information security manuals are present in some hospitals.
23. Incident reporting includes incident handling and management.
24. Archiving is being outsourced in an archiving specialist. Others have internal archiving personnel.
25. Information security clauses are embedded in contracts of job order personnel.
26. System access request form (SAR) shall be used.
27. Document retention policy issued by NAP shall be followed.
28. Upgrading of IT infrastructure is included in the ISSP.
29. IT is the custodian of the security videos

B. Physical Security
    1. Security guards are being outsourced by the hospitals.
    2. Only persons identified should have access to a certain computer. There should be permission to access system from the original user.
    3. Some hospitals are implementing 1 user is to 1 account policy.
    4. Limited access to station should be implemented. Only specific applications intended for use should be stored in the computer.
    5. Only selected offices can use USB. Some hospitals disable use of USB.
    6. Server room is the same with repair room. A dedicated facility shall be put in place for data center.
    7. Role-based access control shall be implemented.
    8. Server should be located in a dedicated room. Office of IT people should be separate from the server room.
    9. No form is being filled out when requesting for the access of the server.
    10. Phone for official use is allocated for communication with healthcare providers relating to patient's treatment.
    11. CCTV, audit trails are put in place to monitor access of IT investments.
    12. Budget allocation for the IT infrastructure of the hospitals contained in the annual financial plan.
    13. Some hospitals have its own security department which covers management of security guards, e.g. viewing of CCTVs.
    14. Head of security is part of the quality committee, and has access to records for traceability purposes.
    15. Regular security audit is put behind in some hospitals.
    16. Server rooms are being accessed by ITs. A dedicated room is put in place.
    17. Systems not dedicated to handle patient information, e.g. mobile phones (smart phones) should not be allowed to be used.
    18. A certain duration shall be implemented for phone orders which shall be put into policy.
    19. Information security measures are not being highly observed in hospitals especially government hospitals.

20. Security education shall be performed among information security personnel of health facilities.
21. Auditing for the completeness of the patient's chart can be done using record completeness chart.
22. Capturing of patient data using camera, etc. should not be permitted.
23. Only one person is in charge of handling the servers.
24. Password expiration can be done.

C. Technical Safeguards
1. Audit logs should be maintained.
2. How to manage contractual relationship shall be included in the IRR.
3. Passwords are changed every month in a certain hospital. It shall be 8 characters in length.
4. RBAC (role-based access) is being implemented.
5. Anti-virus management is being performed.
6. Off-site back up should be put in place.
7. HIS should only be for recording and keeping but access to the MR should be under the MRS.
8. IT people must always adhere to the policy on confidentiality of medical records.
9. LGUs should include data security in the allocation of budget for government hospitals and should also be a priority.
10. There must be identified personnel who can access the IT room, e.g. QA for investigations, HICC for monitoring.
11. MOA for outsourced IT team for hardware management is limited to just job descriptions but no liability is placed on them in cases of adverse events.
12. Access to system is individual.
13. Not enforcing change of password.
14. Back up is done twice a day.
15. Suggestion to include role of DOST-ICTO on information security.

Station 5: General Guidelines and Penalty Clause – Mr. Al Alegre

A. General Guidelines
1. Revised disposal schedule of disposing records DOH no. 70 series 1986
2. Backing up of electronic records, digital storage, archives,
3. Private hospitals - Interim guidelines on disposal on Health/Medical records affected by Typhoon Ondoy issued on Nov 14, 2009
4. Retention of medical records for both government and private health care facilities

B. Penalty Clause
1. Contracts, consultants should be considered, performance matrix,
2. Internal processes; incident reporting, investigation process
3. *Unauthorized processing, authorized processing Philhealth, improper disposal, unauthorized access Reportorial, data subject transparency, negligence,*
4. *Freedom information vs data privacy and data protection*