Electronic Health Record (EHR) Privacy and Confidentiality

مؤسسة حمد الطبية
Hamad Medical Corporation
HEALTH • EDUCATION • RESEARCH صحة • تعليم • بحوث

إدارة معلوماتية التمريض
Nursing Informatics Department

Electronic Health Record (EHR) provides access to each patient's health information and clinical decisions support as well as serves as legal protection both for healthcare providers and patients. Access to and release of patient's information raises concerns involving patients privacy and confidentiality. Nurses and healthcare team members must understand that each person has a responsibility to keep this information secure and private.

Definition Of Terms

The following are some definitions about key concepts in regards to patient privacy and confidentiality.

Privacy
An individual's desire to limit the disclosure of personal health information and avoidance of notice or display.

Security
Measures used to protect the confidentiality, integrity and availability of data and information system.

Confidentiality
Carries the responsibility for limiting the use, disclosure and release of information and can only be permitted with the knowledge and consent of the individual.

Authorization
A special written permission/consent is granted for the use and/or disclosure of a patient's health information or medical records.

Protected Health Information (PHI)
The data that identifies an individual and relates to that person's health, healthcare, or payment for healthcare. PHI can be in electronic, written or oral formats.

KEY CONCEPTS

- **Access to Patient Information**

Information should only be accessed by Hamad Medical Corporation (HMC) authorized professionals involved in patient care. The release of information about the patient is conducted based on HMC policy. At times, information may be required by law, in such cases of medical emergency.

- **Protection of Patient Health Information**

The privacy of patient health information is protected by law. HMC is committed to protecting the confidentiality of our patient record. Healthcare professionals must treat patient's health information with confidence and ensure documentation are saved/stored securely.

- **Safeguards to Protect Health Records**

A few of the safety measures built into Clinical Information Systems (CIS) and used to protect your medical record may include:

- "Access Control" the use of passwords and PIN numbers to limit access to patient information to authorized individuals such as patient's doctors or nurses.
- "Encrypting" stored information. That means health information cannot be read or understood except by someone who can "decrypt" it, using a special "key" made available only to authorized individuals.

Guide To Strengthen Patient EHR Privacy & Confidentiality

Here are some simple guides on how you can preserve privacy and confidentiality of a patient's electronic health record.

- Never share your password to anyone, even a colleague
- Always change your password when compromised or prompted.
- Never leave your computer with open patient's health record unattended.
- Never open suspicious attachments or click unsolicited links as it may lead to phishing and/or a cyber attack.
- Never use your HMC email for personal, non-work related or miscellanous purposes.
- Do not access relatives, co-workers or other health information unless you are authorized.
- Avoid discussing patient's health information in public areas.
- Report any suspected breach of privacy, when in doubt contact your data custodian
- Do not take computer screenshot that containts protected health information (PHI).
- Do not transmit or post any patient related information, image or video by any electronic media that may lead to identification of a patient and degrade or embarrass the patient.
- Do not share or disseminate information gained in the nurse-patient relationship with anyone unless there is a clinical need or legal obligation to do so.
- Avoid printing any protected health information otherwise the physical document must be shredded.

Related HMC Policies

- OP 4042 Privacy, Confidentiality and Access to Health Information
- OP 4086 Information Security
- OP 4105 Password Policy
- OP 4019 Internet Use Policy
- OP 4101 Acceptable Use of HMC Electronic Communication Networks
- OP 4122 Wireless Network Access
- OP 4123 Remote Access Policy

Emphasis on Non Disclosure Agreement

- I will protect the privacy of all clinical, research and business information relating to our patients, research subjects, members, employees, healthcare providers such as patient records, conversations, salaries and communications.
- I know that the confidential information I am exposed to in the course of performing my duties does not belong to me and I have no right of ownership to it.
- I will not misuse confidential information and will access only information necessary to perform my duties.
- I am responsible for my password or misuse of wrongful disclosure or providing unauthorized access to any of HMC's Confidential Information and for my failure to safeguard my access code or other authorization to access Confidential Information.

*Excerpts from HMC Non-Disclosure Agreement

More Information

- iTawasol -> How We Work -> Clinical Services -> Nursing Informatics -> Corporate Nursing Informatics -> Education -> Brochures
- iTawasol -> How We Work -> Corporate Services -> Management of Information
- HIS Gate -> HMC Policies

References

- https://www.healthit.gov/patients-families/faqs/what-security-safeguards-are-designed-prevent-electronic-health-records-being
- http://www.himss.org/library/healthcare-privacy-security
- https://www.hhs.gov/hipaa/
- http://intraappsrv01/POLICIES/hospitals.htm
- http://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf

Contact Us

As advocates for EHR Privacy and Confidentiality, we appreciate and welcome your comments and feedback, Please contact

@ Unit Email: nursinginformatics@hamad.qa

Phone: (+974) 44395201

Fax: (+974) 44395280

17-0528