

## PATIENT PRIVACY AND SECURITY IN EHEALTH

Dr. Güney GÜRSEL

**Department of Medical Informatics** 

Gulhane Military Medical Academy

Ankara/Turkey

**eTELEMED 2015** 





- Definitions
- Patient's rights
- Security and privacy violation Trends
- Consequences of Privacy violations
- Privacy & Security threats
- Solutions to threats
- Laws & Regulations



# **CTARGET**®

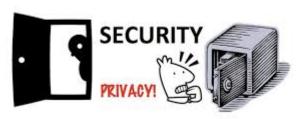




Dr. Güney GÜRSEI eTELEMED2015



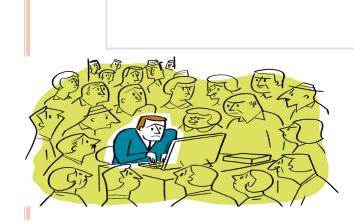






"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite"

Marlon Brondo









- eHealth?
- Privacy?
- Security?
- Patient Privacy and Security?







- Use of information and communication technologies (ICTs)
- o to improve health care
- Used interchangeably with Health Informatics.
- o in the intersection of
  - medical informatics
  - public health
  - business







### Medical Informatics

- Interdisciplinary field
- manages and organizes use of computer technologies
- o to improve health care
- Used interchangeably with Health Informatics



Dr. Güney GURSEL eTELEMED2015





- Freedom from interference or intrusion,
- The right "to be let alone"

• Warren & Brandeis, 1890



- Informational Privacy
- The right to control of access to personal information
  - Moor 1989







- Degree of resistance to, or protection from a threat
  - wikipedia
- Safety or Security?



- Informational Privacy
- The right to control of access to personal information
  - Moor 1989



### Patient Privacy and security

### DEFINITION

- Privacy and security are two different things.
- They are used together as a repetition for patient data.
- In healthcare, these two terms are used together as a concept.
- In which 'Privacy' refers to what is going to be protected
- 'Security' refers to how it will be protected,







- "Whether oral or recorded in any form or medium, that
- is created or received by
  - a health care provider,
  - · health plan,
  - · public health authority,
  - employer,
  - life insurer,
  - school or university,
  - · or health care clearinghouse; and





Health information







o relates to the past, present, or future physical



- or mental health
- or condition of any individual,
- the provision of health care to an individual,
- or the past, present, or future payment for the provision of health care to an individual."
  - HIPAA, 1996



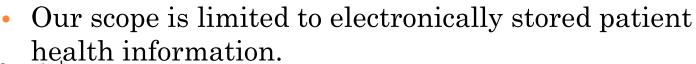


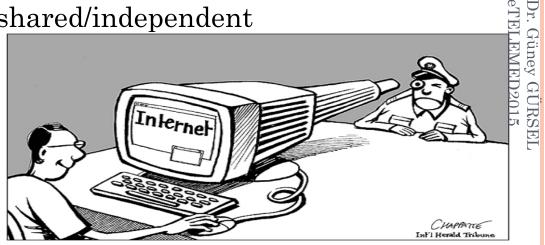


### PATIENT PRIVACY AND SECURITY



- Privacy refers to a general and wide issues
- Private life
- Personal life space shared/independent
- House
- Communication
- Social life
- •
- • • •







Seattle Post-Intelligencer





- Every healthcare organization uses an information system
- Records every piece of patient data electronically
- Facilitates easy access to huge amounts of healthcare data
- Brings some problems and dangers together with the benefits
- One of the biggest dangers is the violation of Patient Privacy and Security



- o In December 2012
- Two Australian radio DJs called a hospital in England
- identified themselves as Queen Elizabeth and Prince Charles
- about a celebrity patient who had been admitted for pregnancy complications





Dr. Güney GÜRSEL eTELEMED2015



- The nurse without veryfing the identities provided them with all the information they asked for
- The Australian DJs were 'on the air' (live program) during that phone call,
- Considering it as a humorous issue,



### **A** DANGER





"UNDER PRIVACY RULES, I CAN'T TELL YOU ANYTHING ABOUT YOUR CONDITION. YOU'LL HAVE TO FIND OUT YOURSELF FROM A MEDICAL WEB SITE."



**A** DANGER

Dr. Güney GÜRSEL eTELEMED2015

- information aw government act product of the project of the projec
- Health data is the most private data of a person
- It can make a person ashamed and upset
- There may be some details even the person himself wants to forget
- Patient Privacy and Security has arisen because of these assets of patient health data.
- Patient Privacy and Security is a challenge to every eHealth application



### **A** DANGER

### Patient Privacy

- Health information privacy; is an individual's right to control:
  - othe acquisition,
  - ouses,
  - or disclosures of his or her
  - 'IDENTIFIABLE' health data

o National Committee for Vital and Health Statistics (NCVHS)







- Protected Health Information ("PHI")
- Electronically Protected Health Information ("PHI")
- "Individually identifiable health information" ("IIHI")



## INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)



- health information,
- including demographic information
- collected from an individual, and:
- '(1) Is created or received by;
- a health care provider,
- health plan,
- employer,
- or health care clearinghouse;





## INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)



- (2) Relates to the past, present, or future
- physical or mental health or condition of an individual;
- the provision of health care to an individual;
- or the past, present, or future payment for the provision of health care to an individual; and







(i) That identifies the individual; or

(ii) There is a reasonable basis to believe the information can be used to identify the individual."

Dr. Güney GÜRSEL eTELEMED2015





## INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)



- o (A) Names;
- (B) All geographic subdivisions
- (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,, discharge date, date of death; and all ages over 89 and all elements of dates
- (D) Telephone numbers;
- o (E) Fax numbers;





# INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)

- (F) Electronic mail addresses;
- (G) Social security numbers;
- (H) Medical record numbers;
- o (I) Health plan beneficiary numbers
- (J) Account numbers;
- o (K) Certificate/license numbers;
- (L) Vehicle identifiers and serial numbers, including license plate numbers;





Dr. Güney GÜRSEL eTELEMED2015

## INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)



- (M) Device identifiers and serial numbers;
- (N) Web Universal Resource Locators (URLs);
- o (O) Internet Protocol (IP) address numbers;
- (P) Biometric identifiers, including finger and voice prints;
- (Q) Full face photographic images and any comparable images; and
- (R) Any other unique identifying number, characteristic, or code





- Disclosure of how PHI is used and protected
- Given copies of their healthcare records
- Request justification of their healthcare records
- Explanation of disclosures made for purposes other than treatment
- Request restriction of the usage and disclosure of his PHI
- File a complaint if he believes privacy rights were





### SECURITY AND PRIVACY VIOLATION TRENDS

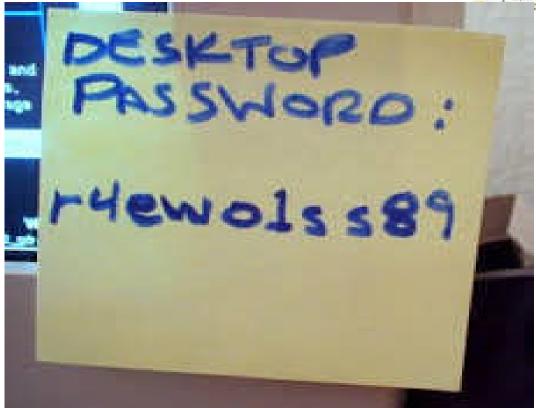


- Advanced persistent threat (APT)
- Malicious attackers
- Data Breaches
- Infinitely distribution possibility of electronic data
- Identity theft
- Ubiquity of digital and mobile devices
- Mistaken dependency on technology















- Loss of money
- Loss of reputation
- Loss of time spent recovering from
- Harm to health
- Even death



















- Identity threats
- Access threats
- Disclosure threats





#### IDENTITY THREATS

- Leaving credentials on public computer
- Sharing passwords
- Insiders mis-use identities to obtain reimbursement (insurance fraud)



Dr. Güney GÜRSEL eTELEMED2015

• Insiders/outsiders mis-use identities to obtain medical services (identity theft)













- The first threat comes from the Patient himself
- Patient has a right to control his PHI
- The Patient can fail to express their consent
- Insiders may "peek" at Patient data, out of curiosity, or with the intent to harm the Patient





### ACCESS THREATS

- o Outsiders may production.

  lead to embarrassment

  o Modification of health records(mistakenly/intentionly)

  Dr. Guney GURSEL

  O Modification of health records(mistakenly/intentionly) • Outsiders may break into Patient records, which may
- - Outsiders
  - Insiders



### DISCLOSURE THREATS

- Data at rest, in the system
- Data at rest, in the mobile devices
- Data in transit







# DISCLOSURE THREATS

- information government act governmen
- Inadvertent disclosure due to
  - Sharing passwords
  - File-sharing tools
  - Malware
- Intentional disclosure
  - For profit
  - For malice









- Authentication
  - Authenticating the Patient
  - Authenticating the provider
  - Authenticating devices
- Anonymity
- Consent Management
- Access Control











- Auditing
- Data integrity
- Secure Transmission
- Device presence









- Health Insurance Portability and Accountability Act (HIPPA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Healthcare Information Management Systems Society
   (HIMSS) privacy and security toolkit







- Enacted in 1996 and updated regularly
- HIPAA privacy rule applies to all forms of patients' PHI, whether electronic, written, or oral
- HIPAA security rule is applied to EPHI only
- Three safeguards for security
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards









- Enacted in 2009
- Strengthened HIPAA's privacy and security guidelines
- Enforces the healthcare organizations to report
  - immediately breaches that affect 500 or more people mandatorily both to HHS and the media
  - less than 500 individuals are supposed to be reported to the HHS on annual basis

    HITECH

Health Information Technology for Economic & Clinical Health Act







- HIMSS has a toolkit for privacy and security
- o Includes 11 major categories, such as;
  - Introduction/Concepts: Basic Foundation Knowledge
  - Laws/Regulations: Local, state, federal, and international
  - Best Practices: Industry produced guidelines
  - Case Studies, Use Cases, Forms and Formats: Real world experiences
  - Personal Health Records: P&S issues unique to PHR
  - o ...









### Data Directive

- 1995 Directive on protection of individuals
- 2002 Directive on the protection of privacy in the electronic communications sector
- 2007 Working Document on the Processing of Personal Dates:
  Relating to Health in Electronic Health Records
- The Prague Declaration -2009









- 2007 Working Document (Data Directive)
  - Explicit Consent
  - Vital Interests
  - Health Professionals (preventive medicine, medical diagnosis)
  - Public Interest









## • The Prague Declaration

- Patient safety and empowerment
- Paying close attention to "legal and ethical issues"
- intent of EU Health Ministers to pay close attention to matters of patient privacy.













matters private.





SENSITIVE DATA Laws & Regulations





Reep your employees' Privacy private healthcare

47







- Eysenbach, G. (2001). What is e-health?. Journal of medical Internet research, 3(2).
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.
- Moor, J. (1989). How to invade and protect privacy with computers. *The information web:* Ethical and social implications of computer networking, 57-70.
- Haux, R. (2006). Health information systemspast, present, future. International Journal of Medical Informatics 75, 268-281.

- o Özturk, H., Bahçecik, N., & Özçelik, K. S. (2014). The development of the patient privacy scale in nursing. *Nursing ethics*, *21*(7), 812-828.
- Lyall S. Prank call seeking royal family secrets takes horrifying turn. New York Times.

  December 7, 2012
- Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. New England Journal of Medicine, 368(11), 977-979.



- HIPAA Act, (1996). Health insurance portability and accountability act of 1996. Public Law, 104, 191.
- Cooper, T., & Collman, J. (2005). Managing information security and privacy in healthcare data mining. In Medical Informatics (pp. 95-137). Springer US.
- Xiong, L. (2012). CS573 Data Privacy and Security Lecture notes. Retrieved June, 25, 2014, from

http://www.mathcs.emory.edu/~lxiong/cs573\_s12/share/slides/0320\_healthcare.pdf



- Kotz, D. A Threat Taxonomy for mHealth Privacy. In Proceedings of Workshop on Networked Healthcare Technology (NetHealth), Bangalore, India, 4 January 2011
- Webb-Morgan, M. (2013, June 12). How to safeguard patient info in the digital age. Article Posted to <a href="http://www.healthcarecommunication.com">http://www.healthcarecommunication.com</a>. Available online at <a href="http://www.healthcarecommunication.com/HIPAA/Articles/How\_to\_safeguard\_patient\_info\_in\_the\_digital\_age\_9857.aspx">http://www.healthcarecommunication.com/HIPAA/Articles/How\_to\_safeguard\_patient\_info\_in\_the\_digital\_age\_9857.aspx</a>
- Center of Medicare & Medicaid Services. (2007). Security 101 for Covered Entities, vol.2, paper 1. Retrieved Jan 10, 2015 from:
  - http://www.http.gov/ocr/privacy/hipaa/administrative/s



- Department of Health and Human Services (HHS) (2009). HITECH Breach Notification Interim Final Rule. Retrieved Jan 30 2015, from http://www.hhs.gov/ocr/privacy/hipaa/understand ing/coveredentities/breachnotificationifr.html
- Healthcare Information Systems Management Society (HIMSS). (2014). Retrieved Jan, 08, 2015, from <a href="http://www.himss.org/">http://www.himss.org/</a>
- o Collman J. & Demster B. (2013). HIMSS Privacy and Security Toolkit Executive Summary.

  Available online at
  - http://www.himss.org/files/HIMSSorg/Content/files/FIToolkit/version6/v7/D01\_Executive\_Sum