The Safety of Medical Information on the Web

PHI
Personal (Protected) Health Information

The concerns of the Governments, and regulatory bodies are regarding the collection, use and disclosure of personal health information, in order to protect the privacy of the individual. These include health status, provision of health care, and payment for health care. But much more as well!

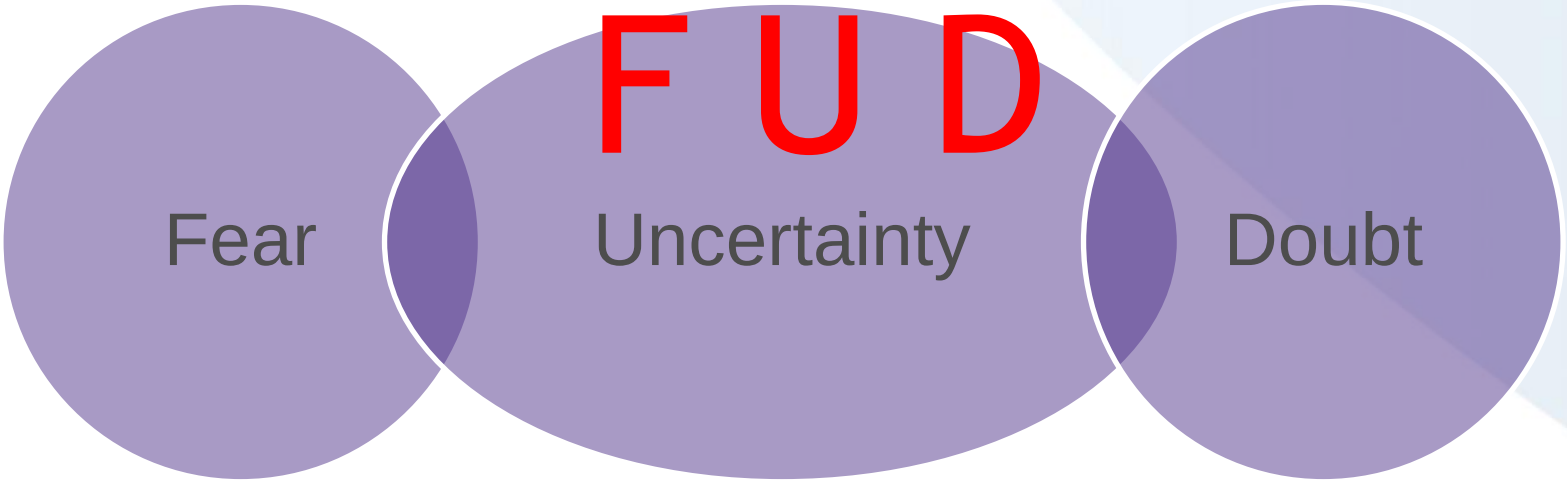
In fact any data which may allow someone else to discover the identity of the individual is also prohibited from being included.

For example: the Health Insurance Portability and Accountability Act (HIPAA) in the States lists 18 “identifiers” which cannot be included in health documents in “clear text”. They must be “tokenized” if included at all.

Names
Geographical identifiers (address)
Dates related to the individual
Phone Number
Fax Number
E-mail
Social Security number
Medical record number
Health insurance beneficiaries
Account number (bank, enterprise, etc.)
Drivers license number
Automobile license plate number
Device identifiers serial numbers
URLs (if they own a web site)
IP addresses
Biometric identifiers, finger, retinal & voice prints
Full face photographs or identifiable images
Unique codes

Statistics

- It takes only 10 minutes to crack a lowercase password that is 6 characters long. Add two extra letters and a few uppercase letters and that number jumps to 3 years. Add just one more character and some numbers and symbols and it will take 44,530 years to crack.
- 73% of Internet users use the same password for all their account access.
- Social media (Facebook, Twitter, etc.) major source for Intelligence gathering by hackers. LinkedIn accounts hacked in June 2013.
- Deloitte recent study of 6 million passwords concluded that 10,000 passwords would open 98% of these e-mail accounts
- E-mail hacking a major target: Yahoo-400,000 e-mails hacked in 2013



What makes Medical Information so special??

One reason is historically, the Hippocratic Oath (late 5th Century BC) every Physician pledges on graduation:

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."

Another reason is regulatory requirements:
USA – Health Insurance Portability and Accountability Act (HIPAA) 1996
USA – The Patient Safety and Quality Improvement Act (PSQIA) 2005
UK – Data Protection Act 1998 – Data Protection Amendment 2003 (Electronic Privacy Regulations)
Canada –Personal Health Information Act 2004 (revised 2010)
European Union Directive 95/46/EC 1995
European countries adopted parts of this such as Germany, France, Holland, etc.

ISO 27799

The International Standards Organization in 2008 renewed an “oldish” standard from 1996 regarding Health Informatics. The purpose of this “standard” is to establish Information Security concepts for the Health Industry.

The Ministry of Health in Israel declared that all Hospitals will be ISO 27799 compliant by December 2013.

Towards the end of 2012 the ISO advisory board began a debate as to whether they should include a recommended standard stating that a Physician cannot give a Nurse or other Physician information regarding treatment verbally at the bed side or in the hallway.

I am pleased to tell you that so far this was deemed unenforceable!

Problems with Regulations

Does HIPAA (or any other regulation) guarantee privacy for my medical information?
No. This is a major misconception about privacy in general. There is no universal privacy rule, even for sensitive medical information. Any privacy you do have depends on a number of things, primarily who has your information.

1992 – Class Action suit of 200,000 women against the manufacturers of the Dalkon Shield intrauterine device. Major problem was getting the Medical Records.

A study of Hospitals adopting Electronic Medical Record systems by MIT Sloan Systems, revealed that Hospitals with a history of malpractice litigation have a reluctance to adopt EMR. The level of recording is too exact and can lead to a more difficult case to defend against.
An example is the case of a patient who was left quadriplegic after surgery. Although the patient initially focused on the surgeon's competence, he switched his focus to the anesthesiologist's competence after the EMR showed a time-stamp that cast doubt on whether the anesthesiologist was present for the entire procedure.

Who Steals Medical Information?

This is a very insidious form of fraud, Identity Theft, which occurs when a criminal steals your personal information and uses it to obtain medical services. They will use your identity and insurance to seek medical attention, have expensive operations or, give birth — leaving the bill in your name.
In doing so, they will have altered your vital medical information (blood type, allergic reactions etc.) which can be potentially fatal to you.

Thieves – insurance scams, fraud
Drug Addicts – to purchase prescription drugs
Enemies – vindictive acts to harm your reputation and your pocket
Newspaper reporters - information
Insurance companies - to deny paying

Criminal Services offered for a fee APT…. The world of Cyber

The prediction is that in 2014 APT, a Cyber hack, will be offered for a fee. Professional hackers will offer to hack anything for a fee and give you a guarantee of success.

Mitigation of the Threats

WWW = Wild Wild West, enter at your own risk, be very cautious & suspicious – you may be liable for leaking medical information!

Security Awareness is the number 1 mitigation. If you recognize the need for privacy then you will be willing to accept a slightly less intuitive experience:

- Encrypting the e-mail
- Sending the files to a SFTP server requiring access control to download the information
- Using ‘Vaults’ in place of ‘Dropboxes’
- Do not keep any data (e-mails, files, etc.) in your Phone or laptop or even Home PC which are not protected!
- Mobile devices should be equipped with Anti Virus/Malware/Phishing software as well as ‘wipe’ software in the event of loss or theft.
- Connecting to Public WiFi is opening a door to a hacker and inviting him/her in!