R.A. 10173 (DATA PRIVACY ACT OF 2012) AND BEYOND

privacy, technology, & public policy in electronic health management

ALAN G. ALEGRE
Foundation for Media Alternatives

fma @25

PHIC Workshop
24 April 2014 | Privato Hotel, Pasig

Roadmap

1. **Locating Privacy Rights in "Digital/Information Societies"**
   > privacy, security, and technology
   > towards privacy protections
   > defining privacy: informational privacy

2. **Introducing RA 10173: Data Privacy Act of 2012**

3. **Health Information Privacy: Some Implications**

Locating “Privacy”

The privacy milieu

- **Complicated area of discourse**

  Affects us in the roles we play in society:

  citizen, consumer, friend, family member, traveller, medical patient, partner…and what we do everyday

- **Rising significance in the policy arena: public interest**
  - Changing SECURITY environment >> Governments collecting more information: 'anti-terror, 'anti-crime'
  - Changing ECONOMIC environment Private companies collecting more
  - Evolving communication habits: "Always available"; ubiquity of devices, significance of ICTs/internet in personal/professional life:
  - Partly due to technological change >> Implications on HOW WE CAN BE TRACKED (Surveillance)

What information we disclose, to whom we disclose it, and how

Privacy & Technology

Rise of privacy discourse due to devts in technology

- **New surveillance techniques > new privacy concerns**
  - **Privacy as a RIGHT** in late 19thC (Brandeis*: "right to be left alone")*: development of the camera & tabloid journalism
  - comms surveillance by govt in the 1950s: anti-wiretapping laws
- **ANALOG > DIGITAL: Advanced databases data analysis** (60's-70s) – signalled the development of many privacy laws
- **Now: DATA-RETENTION, DATA-MINING >> cloud, big data…**
  - Vast amounts of personal info collated: variety of sources
  - Subjected to powerful programs/algorithms to predict behavior
  - + Web 2.0: Explosion of SOCIAL MEDIA

Privacy & Technology

CURRENT INTERNET ECOSYSTEM: "Google & Facebook, Snowden & Surveillance"

> **The INTERNET is MOBILE...MOBILE is SOCIAL**

> **Post-PC World, Cloud Computing, Big Data...**

> Social Media: NOTHING GETS DELETED?!

- Searches, emails, browsing histories >> Behavioral advertising

INQUIRER TECHNOLOGY | INQUIRER NEWS

HOME | NEWS | SPORTS | LIFESTYLE | ENTERTAINMENT | BUSINESS | TECHNOLOGY

HEADLINES | LATEST TECHNOLOGY STORIES | BLOGS

Latest Stories: Palace on 'Noynoying': Creative but no effect

Home > Technology > Latest Technology Stories > Apple, Google defend privacy practices before US Congress

Apple, Google defend privacy practices before US Congress

By: Chris Lefkow
Agence France-Presse
11:19 am | Wednesday, May 11th, 2011

+1 0 | Tweet 0 | share New | Share 0 | Recommend

WASHINGTON—Apple and Google, facing questioning from skeptical US lawmakers, defended their privacy practices before a congressional committee on Tuesday.

Privacy watchdog says Google breaks data law

Thomas Escritt, Reuters · Friday, November 29, 2013 · 6:57 am

Share | Tweet 6 | Like | 16 people like this. Be the first of your friends.

Google's practice of combining personal data from its many different online services violates Dutch data protection law, the country's privacy watchdog said on Thursday after a seven-month investigation.

The Dutch Data Protection Authority, or DPA, asked Google to attend a meeting to discuss its concerns, after which it would decide whether to take any action against the cloud services, Internet search and advertising giant, which could include fines.

Google, responding to the Dutch authority's findings, said it provided users of its services with sufficiently specific information about the way it processed their personal data.

Towards Privacy Protections

- Earlier HR and consti rights: **privacy overlooked**
- **NOW: broadly regarded as a FUNDAMENTAL HUMAN RIGHT**
  - **e.g., Constitutional/supreme courts**
    Part of "human dignity" (Germany, Ireland), "freedom of expression (US)", "right to liberty" (IN, JP), protection of "personality" (Norway); "general duty of confidence" (SG)
- **Recent constitutional and legal frameworks: more explicit**
  Patterned after INTERNATIONAL CONVENTIONS
  - Universal Declaration of Human Rights (UDHR)
  - Intl Convention on Civil & Political Rights (ICCPR)
  - EU Convention on HR
  - Gender: CEDAW

Towards Privacy Protections

- **Constitutional guarantees** (uneven across countries)
- **Privacy Laws: general/sectoral**
  - **In response to abuse:** incidents > media coverage > public concern legislative inquiry + media attention
  - **Legislative action** (e.g., RA 9995 "*Cyberboso*" Act post-Kho-Halili)
  - **Jurisprudence:** court decisions form a body of rules
- **"FAIR INFORMATION PRACTICES"**
- **Some legal protections, but approach is often piecemeal and uneven**
  - e.g., **privacy of communications** viz. **privacy of medical records?**
  - e.g., **regulation of financial sector** viz **regulation of marketing & advertising industries?**

DEFINING PRIVACY

- **Of all HRs: probably most difficult to pin down**
  Wide variation: context & environment
- **Some perspectives:**
  - Brandeis: individual's "right to be left alone"
  - Robert Ellis Smith: "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves"
  - **Westin: the claim of an individual to determine what information about him/herself should be known to others**
  - **International Telecommunications Union: right of individuals to control or influence what information related to them may be disclosed.**
  - **The absence of (unreasonable) intrusion, surveillance, monitoring, tracking, oversight etc**

DEFINING PRIVACY

DIMENSIONS/ASPECTS OF PRIVACY

- Communications privacy
- Physical/Bodily privacy
- Territorial privacy
- Locational privacy
- Decisional privacy
- Informational privacy
  (a.k.a., DATA PROTECTION)*

* A right/interest in its own; instrumental in the delivery of most other dimensions, where RECORDS are created

2.
Data Privacy Act of 2012
R.A. 10173

National Context

- **PH lacked a comprehensive law on data protection**
  - Existing laws on privacy of information are largely sectoral or otherwise specialized or limited in scope.
  - No law that sets down the State policy and principles of data protection as a distinct concept of privacy.
  - No law that lays down the rights of the individual as data subject and provides a mechanism for enforcing the same (i.e., penalizing violations).
- **A comprehensive law will have standard- or normsetting functions and educative functions.**
- **Comprehensive laws may lay or strengthen the foundation of sectoral laws.**

Data Privacy Act of 2012

"An Act protecting individual personal data in information and communication systems in the government and the private sector, creating for this purpose a National Privacy Commission, and for other purposes."

- **RA 10173**
  - Senate Bill No. 2965 & House Bill No. 4115
  - Originally modelled after EU data protection laws; moving towards APEC model (Privacy Principles)
  - Filed during 14th Congress; re-filed 2010
  - Signed into law 15 August 2012 > unimplemented
    No IRR yet > Natl Privacy Commission not yet appointed

R.A. 10173 : Data Privacy Act of 2012

STATE POLICY:

The State shall protect the
FUNDAMENTAL HUMAN RIGHT OF PRIVACY …
while ensuring the free flow of information
to promote innovation and growth.
It has the inherent obligation to ensure that
personal information in information & communication
systems—in the government and private sector—
are secured and protected.

Data Privacy Act of 2012

Key Terms:

- Personal Information
- Sensitive Personal Information
- Privileged Information
- Processing; Personal Information Processor
- Personal Information Controller

Data Privacy Act of 2012

Terms:

- **PERSONAL INFORMATION**

  any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably ascertained by the entity holding the information, or when put together with other information would identify an individual

PERSONALLY IDENTIFIABLE INFORMATION

Data Privacy Act of 2012

Terms:

- **SENSITIVE PERSONAL INFORMATION**

  personal information:

  - about a person's race, ethnic origin, color, and religious, philosophical or political affiliations
  - about a person's health, genetic, or sexual life, or any judicial proceedings for any offense committed or alleged to have been committed by such person
  - issued by gov't agencies (social security numbers, health records, licenses, tax returns)
  - established as classified by law

Data Privacy Act of 2012

Terms:

- **PRIVILEGED INFORMATION**

  any and all forms of data that constitute privileged communication under the Rules of Court and other laws

Data Privacy Act of 2012

Terms:

- **PERSONAL INFORMATION CONTROLLER**

  a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his/her behalf, BUT excluding the person or organization so instructed

Data Privacy Act of 2012

Terms:

- **PROCESSING;**

  Personal Information Processor

  any operation or set of operations performed upon personal information, including collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data

Data Privacy Act of 2012

GENERAL RULES

Personal information is private, hence, protected.

Processing of personal information is allowed, subject to legal requirements and adherence to general data privacy principles.

Processing of sensitive personal information and privileged information is prohibited, with certain exceptions.

Data Privacy Act of 2012

GENERAL RULES

Processing of personal information is allowed, subject to legal requirements and adherence to general data privacy principles.

- Transparency
- Legitimate purpose
- Proportionality

Data Privacy Act of 2012

KEY SECTIONS

- General Provisions: Scope (Ch. I)
- National Privacy Commission (Ch. II)
- General Data Privacy Principles
  Processing of Personal Information
  (Ch. III)
- Rights of the Data Subject (Ch. IV)
- Security of Sensitive Personal Information (Ch. V)...
  in Government (Ch. VII)
- Penalties (Ch. VIII)

Data Privacy Act of 2012

SCOPE:

Applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found and established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines ....

Chapter I. General Provisions

- **Sec 4. Scope**

  The Act does not apply to :

  – Information about an officer or employee of a government institution
  – An individual performing work under contract for a government institution
  – Relating to a benefit of financial nature
  – Information processed for journalistic, artistic, literary or research purposes
  – Necessary to carry out functions of a public authority
  – Information collected from foreign jurisdictions

Chapter I. General Provisions

- **Sec 5. Protection afforded to journalists and their sources**
- **Sec 6. Extraterritorial application**
  - Information about a Philippine citizen or resident
  - Entity has a link with the Philippines (e.g. contract, local central management and control , branch/office/ subsidiary)

Chapter II. The National Privacy Commission

- **Sec 7. Functions of the NPC**

  An independent body
  Act as a collegial body
  Has quasi-judicial, regulatory powers

- **Sec 8. Confidentiality**
- **Sec 9. Organizational structure**
- **Sec 10. Secretariat**

Chapter II. The National Privacy Commission

- To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection.
- Ensure compliance of personal information controllers
- Monitor compliance of government entities on their security and technical measures (to meet minimum standards)
- Receive complaints, institute investigations, facilitate/ enable settlement of complaints, adjudicate/award indemnity, prepare reports/publicize
- Recommend to DOJ: prosecution & penalties
- Review, approve, reject or require modification of privacy codes of PICs

Chapter II. The National Privacy Commission

Organizational Structure

- Privacy Commissioner (Chair) – rank of Secretary
- Deputy Privacy Commissioner - Data Processing Systems
- Deputy Privacy Commissioner - Policies and Planning

- Appointed by the President for a term of three (3) years and may be reappointed for another 3-year
- Must be recognized experts in ICT and data privacy

- (Attached to a Dept of ICT) >> Office of the President Secretariat to be established: majority composed of govt data handlers who have served at least 5 years

Chapter III.
Processing of Personal Information

- **Sec 11. General data privacy principles**

  Personal information must be :

  – Collected for specific and legitimate purposes
  – Processed lawfully
  – Accurate and relevant, up-to-date
  – Adequate and not excessive
  – Retained only for as long as necessary
  – Permits identification of data subjects for no longer than is necessary

Chapter III.
Processing of Personal Information

- **Sec 12. Criteria for lawful processing of personal information**
  - Consent
  - Fulfillment of a contract
  - Compliance with a legal obligation
  - Protection of life and health of data subject
  - Response to a national emergency, public order and safety
  - Legitimate interests, subject to rights of data subject

Chapter III.
Processing of Personal Information

- **Sec 13. Sensitive personal information and privileged information**

  Processing is prohibited, except when :

  - Data subject has given consent
  - Processing is provided by existing laws
  - Necessary to protect life and health of data subject
  - Necessary to achieve lawful and noncommercial objectives of an organization + no transferring to 3rd parties, consent
  - Necessary for medical treatment, and adequate level of protection is ensured
  - Necessary for the protection of lawful rights and interests in court proceedings

Chapter III.
Processing of Personal Information

- Sec 14. Subcontract of personal information
- Sec 15. Extension of privileged communication

Chapter IV. Rights of the Data Subject

- **Sec 16. Rights of the data subject**
  - **Be informed when personal information shall be, are being, or have been processed**
  - **Be furnished the information :**
    - Description of the information
    - Purposes
    - Scope and method
    - Recipients
    - Methods utilized for automated access

    + **Access** to the above, upon demand
  - **Dispute inaccuracy or error**
    - Suspend, withdraw, order blocking, removal, or destruction
    - Be indemnified

Chapter IV. Rights of the Data Subject

Generally, the data subject is entitled to know:

1) if his/her personal information is being processed;
2) what the processed information concerns;
3) why it is being processed;
4) how, and to what extent, it is being processed;
5) to whom it may be disclosed;
6) the extent of automated access (if applicable);
7) the identity and contact details of the personal information controller;
8) how long it is going to remain stored; and
9) his/her specific rights under the Act.

Chapter IV. Rights of the Data Subject

- **Sec 17. Transmissibility of rights of the data subject**
- **Sec 18. Right to Data Portability**
- **Sec 19. Non applicability**
  - The immediately preceding sections are NOT applicable when used only for scientific and statistical research and no activities are carried out and no decisions are taken regarding the subject
  - Provided information is held under strict confidentiality and used only for the declared purpose
  - Criminal, administrative, tax liabilities

Chapter V. Security of Personal Information

- **Sec 20. Security of personal information**
  - **Reasonable and appropriate organizational, physical, and technical measures to protect personal inf**o vs accidental/unlawful destruction, alteration and disclosure, and any other unlawful processing
  - **Integrity vs. natural dangers:** accidental loss or destruction
  - **Protection vs human dangers**: unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination
  - **Security measures: extends to 3rd parties**
  - **Notification**: DPC and subject in case of breach

Chapter VI. Accountability for Transfer of Personal Information

- **Sec 21. Principle of Accountability**
  - PIC responsible (incl. info transferred to 3rd parties)
  - PIC to designate individual/s accountable for organization's compliance with this Act; identity shall be made known to data subject upon request

Chapter VII. Security of Sensitive Personal Information in Government

- **Sec 22. Responsibility of heads of agencies**
- **Sec 23. Requirements relating to access by agency personnel to sensitive personal info**
  - On-site and online access
  - Offsite access prohibited unless subject to guidelines: deadline for approval/disapproval by HoA; limitation to 1,000 records; encryption
- **Sec 24. Applicability to government contractors**

Chapter VIII. Penalties

> 1 to 6 years imprisonment

> Php 500,000 to Php 4Million

Sec 25. Unauthorized processing

Sec 26. Accessing due to negligence

Sec 27. Improper disposal

Sec 28. Wrongful processing: unauthorized purposes

Sec 29. Unauthorized access or intentional breach

Sec 30. Concealment of security breaches

Chapter VIII. Penalties

- Sec 31. Malicious Disclosure
- Sec 32. Unauthorized Disclosure
- Sec 33. Combination of series of acts
- Sec 34. Extent of liability
- Sec 35. Large scale
- Sec 36. Offense committed by public officer
- Sec 37. Restitution

Chapter IX. Miscellaneous Provisions

- **Sec 38. Interpretation**
- **Sec 39. Implementing Rules & Regulations (IRR)**
  - **NPCommission to promulgate IRR within 90 days of effectivity**
- **Sec 40. Reports and Information**
- **Sec 41. Appropriations Clause**
  - **Initial PhP20 Million; PhP 10M/year for 5 years**
- **Sec 42. Transitory Provision**
- **Sec 43. Separability Clause**
- **Sec 44. Repealing Clause**
- **Sec 45. Effectivity Clause**

IN CONCLUSION

- **PH now has a comprehensive data protection law**
  - Imperfect, but sufficient: SUPPORT for the law
  - IMPLEMENT! Appoint DPC & promulgate IRR (address imperfections: exemptions & criteria, data-retention, data-subject consent, etc…)
  - Strategize other executive issuances (ICTO) + Department Orders
  - Strategize key sectoral or supplementary laws or amendments: e.g. health info privacy, anti-wiretapping; gender-related laws
- **Need to embark on a strategic awareness-raising effort: multi-stakeholder**
- **Alignment with international standards**: ongoing effort especially in new areas (esp. with technology)

3. Health Information Privacy: Some Implications

Health Info Privacy Policy Paper (2013)

Principal Investigator

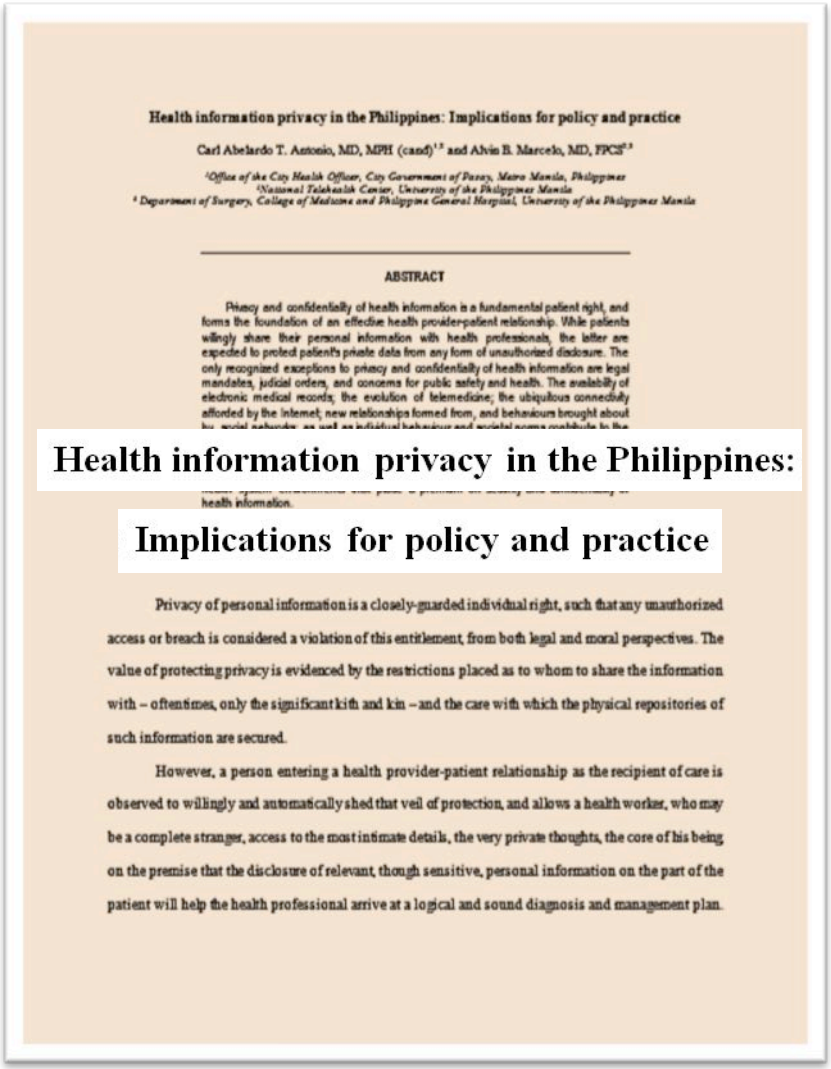
- **Dr. ALVIN B. MARCELO**

Privacy Consultant

- **Dr. CARL A. T. ANTONIO**

Legal Consultant

- **Atty. IVY D. PATDU M.D.**



Health information privacy in the Philippines: Implications for policy and practice

Carl Abelardo T. Antonio, MD, MPH (cand)[1,2] and Alvin B. Marcelo, MD, FPCS[2,3]

[1]Office of the City Health Officer, City Government of Pasay, Metro Manila, Philippines
[2]National Telehealth Center, University of the Philippines Manila
[3] Department of Surgery, College of Medicine and Philippine General Hospital, University of the Philippines Manila

ABSTRACT

Privacy and confidentiality of health information is a fundamental patient right, and forms the foundation of an effective health provider-patient relationship. While patients willingly share their personal information with health professionals, the latter are expected to protect patient's private data from any form of unauthorized disclosure. The only recognized exceptions to privacy and confidentiality of health information are legal mandates, judicial orders, and concerns for public safety and health. The availability of electronic medical records, the evolution of telemedicine, the ubiquitous connectivity afforded by the internet, new relationships formed from, and behaviours brought about

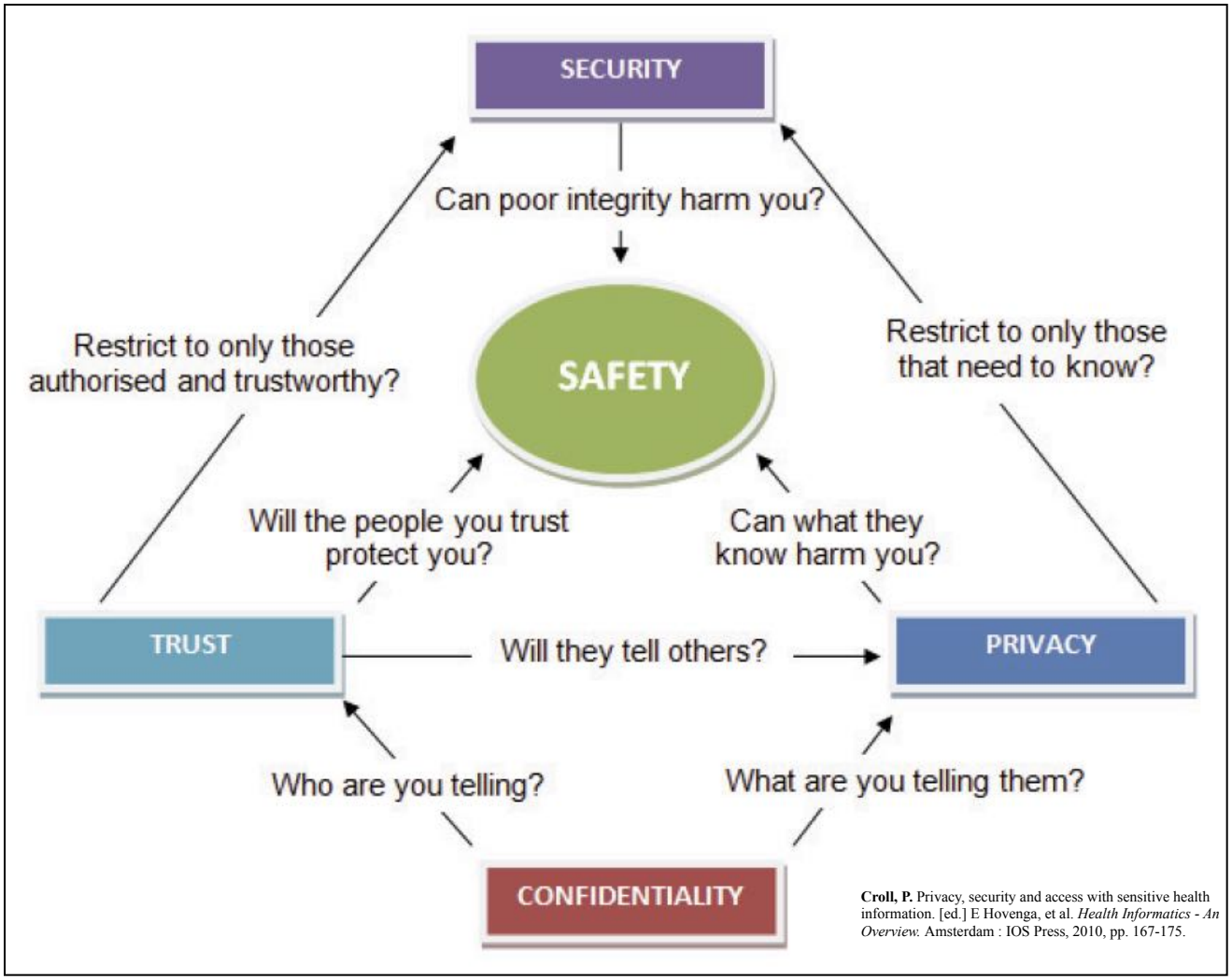
Health information privacy in the Philippines:

Implications for policy and practice

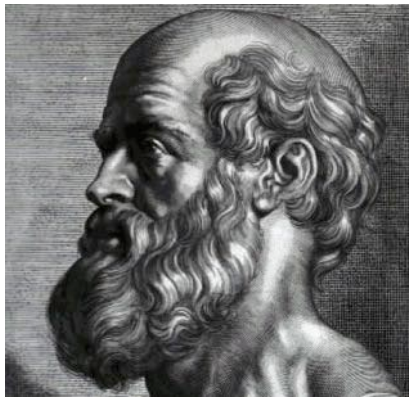
Privacy of personal information is a closely-guarded individual right, such that any unauthorized access or breach is considered a violation of this entitlement, from both legal and moral perspectives. The value of protecting privacy is evidenced by the restrictions placed as to whom to share the information with – oftentimes, only the significant kith and kin – and the care with which the physical repositories of such information are secured.

However, a person entering a health provider-patient relationship as the recipient of care is observed to willingly and automatically shed that veil of protection, and allows a health worker, who may be a complete stranger, access to the most intimate details, the very private thoughts, the core of his being on the premise that the disclosure of relevant, though sensitive, personal information on the part of the patient will help the health professional arrive at a logical and sound diagnosis and management plan.

Privacy & healthcare: A centuries-old affair



Croll, P. Privacy, security and access with sensitive health information. [ed.] E Hovenga, et al. *Health Informatics - An Overview.* Amsterdam : IOS Press, 2010, pp. 167-175.



"All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."

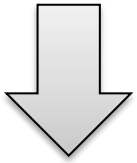
Hippocrates, 4th Century BC

Slide from Dr Carl Antonio

PRIVACY & CONFIDENTIALITY
Two sides of the same coin

Privacy

The state of being free from intrusion or disturbance in one's private life or affairs.

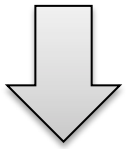


RIGHT

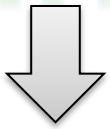
Patients

Confidentiality

The privacy of information and its protection against unauthorized disclosure.



DUTY



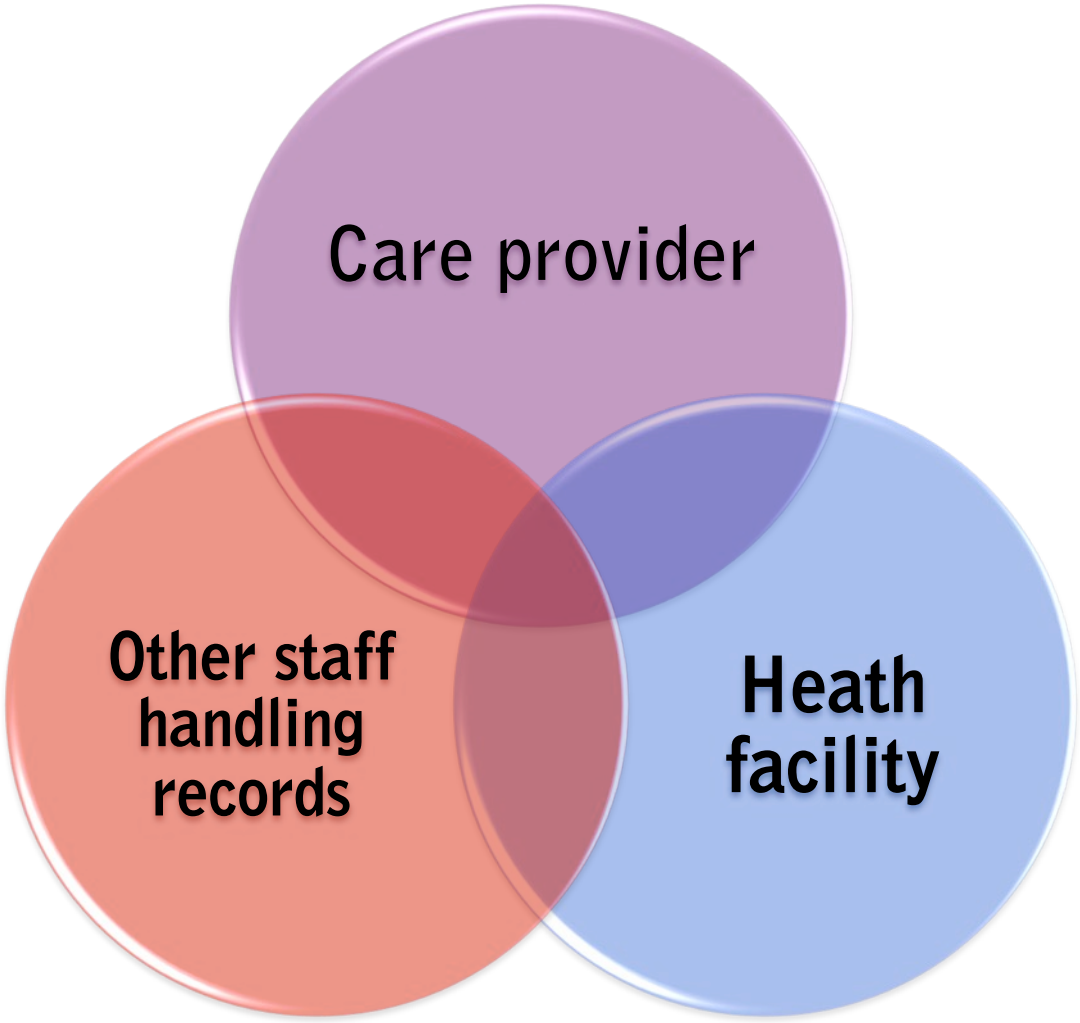
Care Providers

Right to privacy is guaranteed by the Constitution and protected by existing laws

In General	Professionals	Institutions	Special Cases
• 1987 Constitution • Civil Code of the Philippines • Revised Penal Code • + RA10173	• The Medical Act of 1959 • Rules of Court • *Lim vs. Court of Appeals* • *Krohn vs. Court of Appeals*	• DOH Licensing • PHIC Benchbook • *Professional Services, Inc. v. Agana*	• HIV/AIDS (RA 8505) • Drug Rehab (RA 9165) • VAWC (RA 9262)

Slide from Dr Carl Antonio

Confidentiality of health information is recognized



Duty-bearers of confidentiality

Duty to maintain confidentiality not only rests with the medical provider but extends to:

- the hospital or health facility
  - Ng & Po (2006)
  - Bellosillo et al (2010)
- all persons involved in handling and maintaining patient records
  - RA No. 8504

Slide from Dr Carl Antonio

But the system is not fool-proof

Palace makes a clean breast of Arroyo implant

By TJ Burgonio
Philippine Daily Inquirer
First Posted 04:30:00 07/04/2009

Filed Under: Health, Politics

MANILA, Philippines ? A ?boob jo
NO way!

After initially denying President G
had breast implant, Malacañang h
that she underwent such a medic
80s.

The Palace also confirmed that M
conducted on lumps found on her
on a two-day self-quarantine at th
Medical Center early this week. T
biopsies were normal, according

Video scandal grips Cebu hospital

By Carine M. Asutilla
Cebu Daily News
First Posted 14:07:00 04/15/2008

florist in his 30s
s surgery for the

atic.

of sex with a stranger was

he surgery three months
Tube.

medical personnel at the
er (VSMMC).

Vaginismus: When vaginal muscles contract

abs-cbnNEWS.com
Posted at 09/13/2010 1:12 PM | Updated as of 09/14/2010 12:17 PM

Tweet 17 Recommend 372 +1 0

MANILA, Philippines - **Rumors** saying that local celebrity couple--John Lloyd Cruz and Shaina Magdayao--was rushed to a hospital after suffering from what is called *penis captivus* has been denied by Star Magic.

Simply put, the so-called condition refers to an instance when a woman's muscles in the vagina clamp down on a man's penis so firmly that they lock inseparably in sexual intercourse.

Penis captivus is said to be common among animals (such as dogs), but not humans. The so-called condition may have a "largely hearsay" existence in medical history but is "not entirely mythical," a study by the British Medical Journal (BMJ) showed.

"Such a reaction cannot be dismissed offhand as impossible. It is theoretically quite possible. Yet it does not seem to have occurred in the past 100 years or so," BMJ said in the **study**, which was released in 1979.

Evolution of technology = Change in the landscape of privacy in healthcare

Slide from Dr Carl Antonio

Clinical care deals with a variety of sensitive areas

- Psychiatric care… Treatment of juveniles…
- Obstetrics/Gynecology…
- Cancer Therapy…
- VIP hospitalizations…
- Episodes of Sexually Transmitted Diseases…
- Genetics Information…

+ other domains: medical research, medical education, public health reporting, other legal & regulatory requirements…

Some Privacy & Confidentiality Issues

Some Issues/Concerns in Health Info Privacy

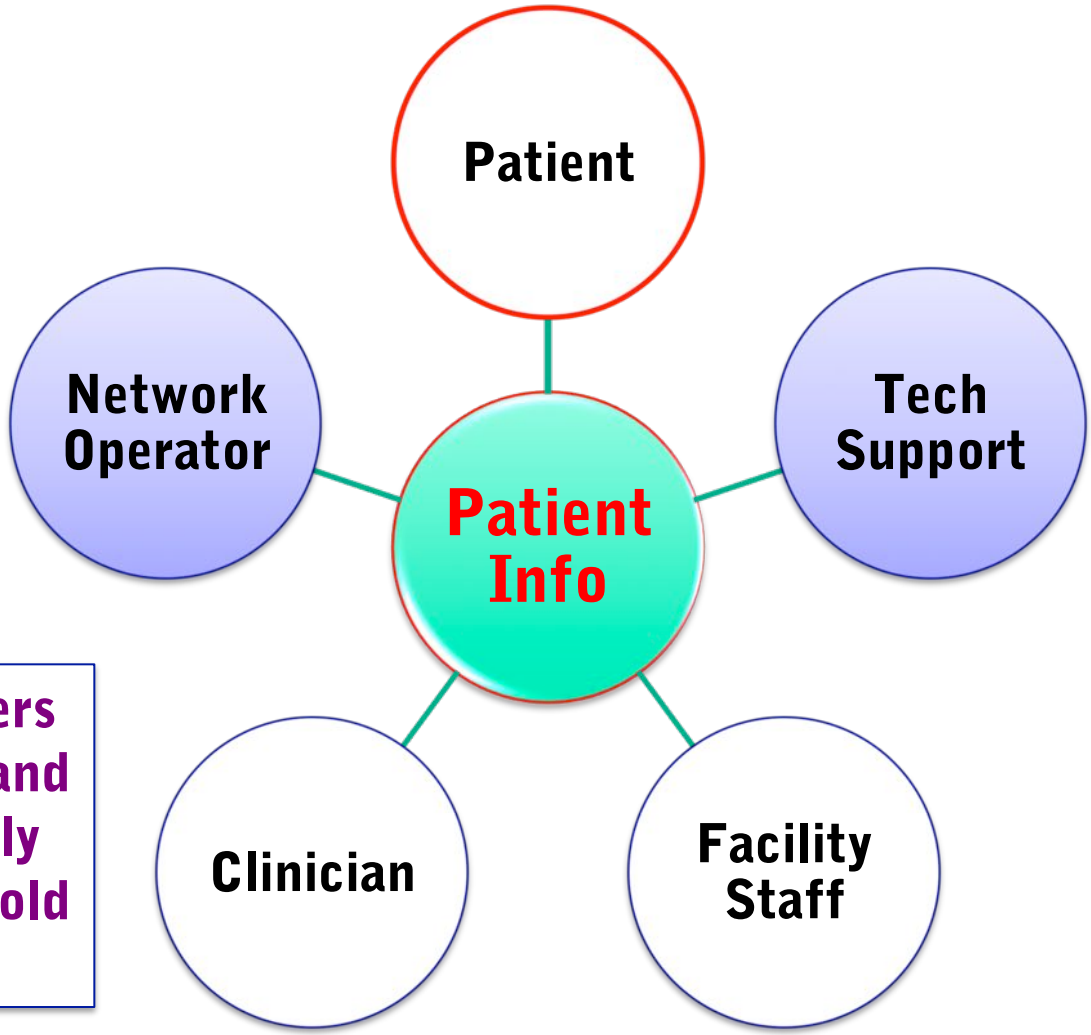
- No specific policy frame specific to Health Information Privacy and Technology
- Non-health professionals have access to patient records
- Multiple access points for health information
- Use of ICT by healthcare professionals: Ethics and Regulation
- Role of 3rd party intermediaries: PII transmitted through telcos/ISPs?
- Socio-cultural practices of health care in the Philippines

- **Some concerns in could be addressed by RA 10173; need specifics… participation in the IRR development**
- **Need for a sectoral framework and supplemental policy issuance/s (e.g., US HIPAA, NZ HealthInfo Privacy Code)**

Slide from Dr Carl Antonio

Privacy and Confidentiality Issues with Health IT:

Access to patient records

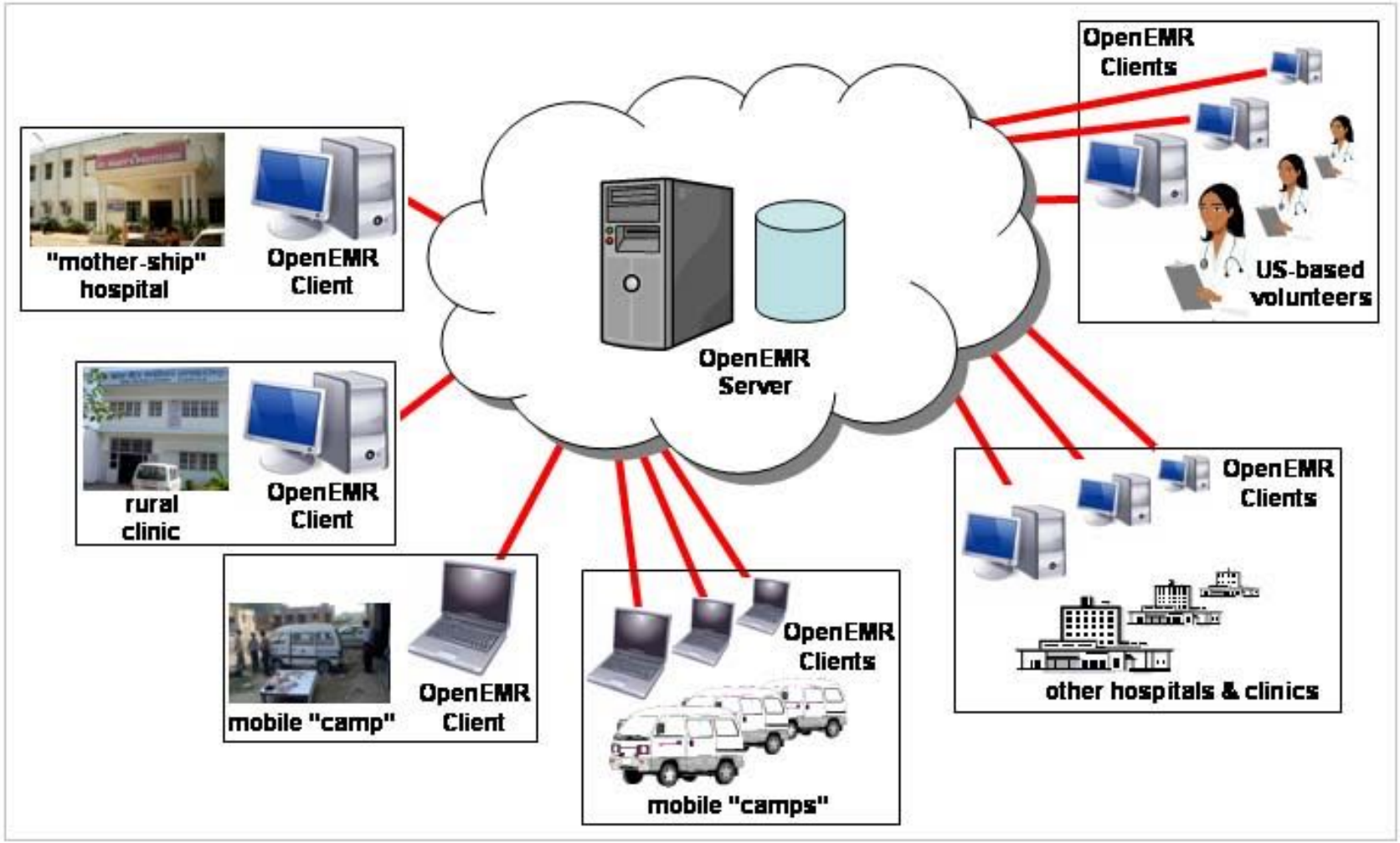


Should non-health professionals involved in handling of patient data be similarly bound by codes of ethics?

Health workers are ethically and professionally bound to uphold privacy.

Privacy and Confidentiality Issues with Health IT

Multiple Access Points for Health Information



Slide from Dr Carl Antonio

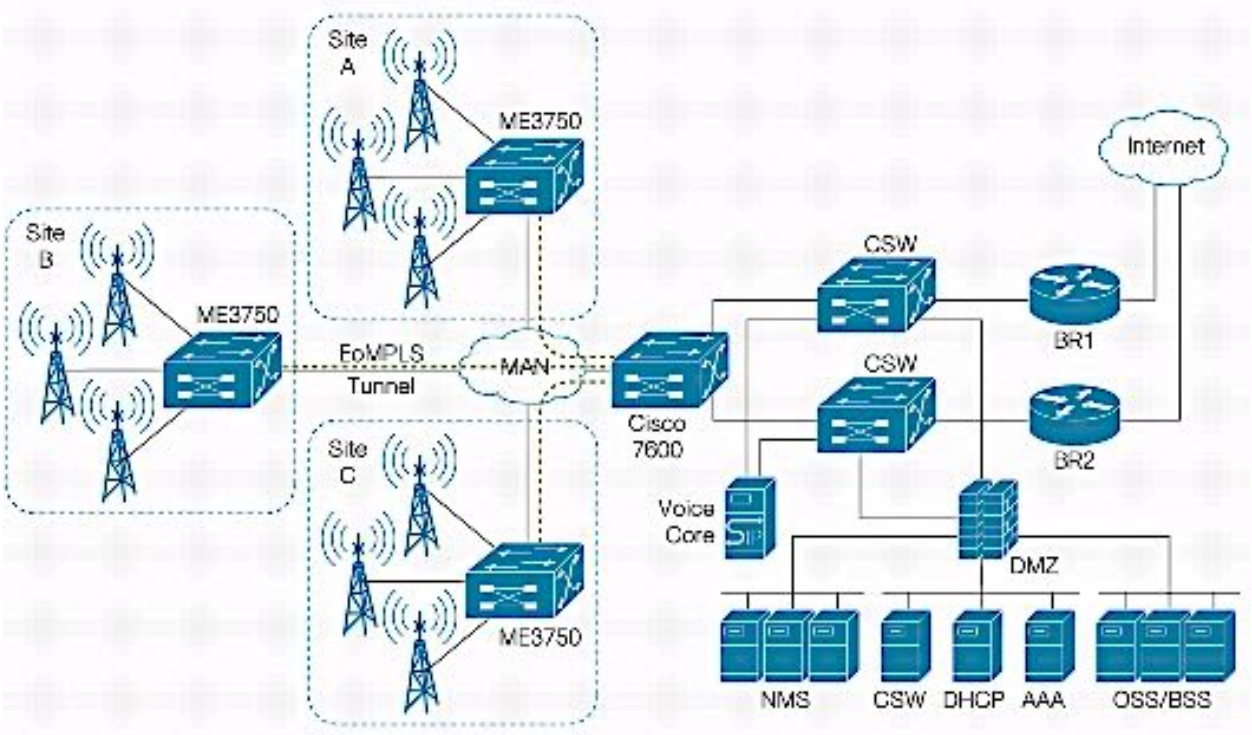
Privacy and Confidentiality Issues with Health IT

Multiple Access Points for Health Information

Cloud-based EMRs

Telemedicine consult

Electronic referrals



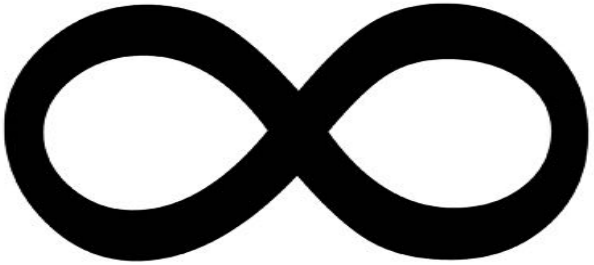
- **Privacy policies of telcos/ISPs not uniform**
- **NTC oversight may be inadequate**

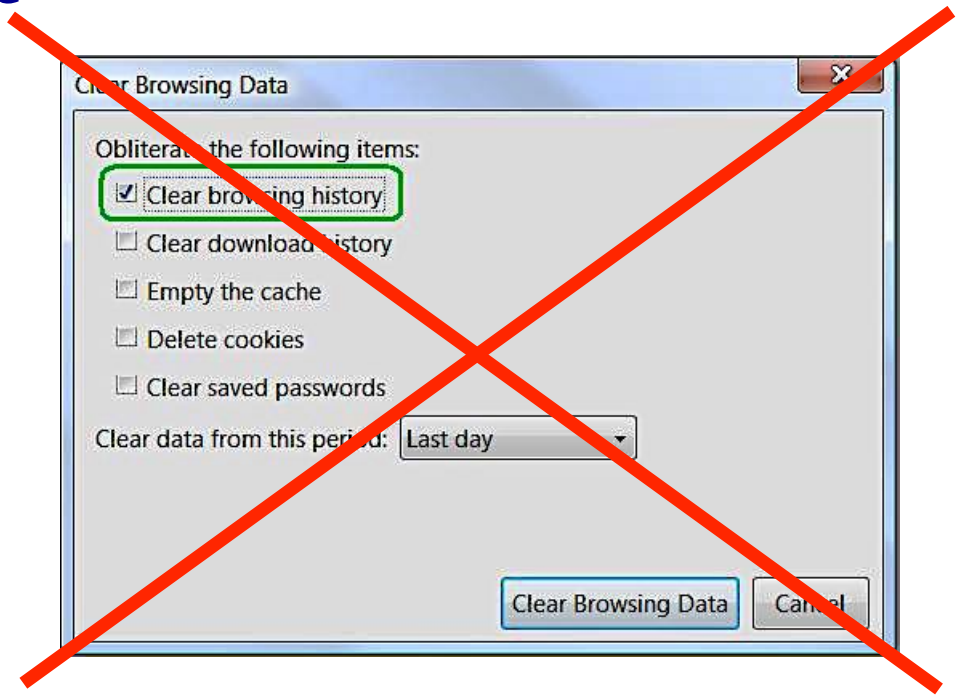
Initial findings of privacy mapping of telcos by FMA.

Slide from Dr Carl Antonio

+ Infinite Data Lifespan on the Internet…

- **Data transmitted through electronic channels are stored indefinitely and permanent deletion may be impossible.**





Security Elements of the Privacy Framework

- **Physical security**
- **Electronic security**
  - Data in transit
  - Data at rest
- **Procedural security**
- **Ethical and legal considerations & codes**
  - Data release policies and procedures

Privacy & Security in agencies/institutions

Administrative

- Institution has written policies
- Training
- Addressing issues, e.g. security breaches

Physical

- Workstation placement/use
- Control Re: access to hardware, software

Technical

- Role-based access control
- Data encryption
- Authentication

Some implications for health care professionals

- **Privacy by Design: ALL health info**
  - **Policies & protocols**: information life-cycle
  - **Leadership**: Privacy (compliance) 'officer' (CIO?)
  - **Monitoring & Compliance Framework:** process & guidelines
- **Policy & Standards Development in the health sector**
  - Rights of Data Subjects: informed **consent**, **NDAs**, provisions for **acceptable use**, guarantees **vs repurposing >** TORs, forms, templates
  - **Anonymization/de-identification** when necessary
  - **International benchmarking…**
  - **Data Security!** – to protect against breaches
- **Orientation/Capacity-Building of Stakeholders**
  - Data Handlers: Medical Staff, Research Team/s & Technical Team/s
  - Data subjects: students, research subjects…
  - 3rd Party providers/outsourced services

TOWARDS A UNIFIED HEALTH INFO POLICY

Model Instruments

- Health Information Privacy Code (New Zealand)
- Privacy Act of 1998 (Australia)
- Pan-Canadian Health Information Privacy and Confidentiality Framework
- Health Insurance Portability and Accountability Act + HIPSA & HITECH (USA)

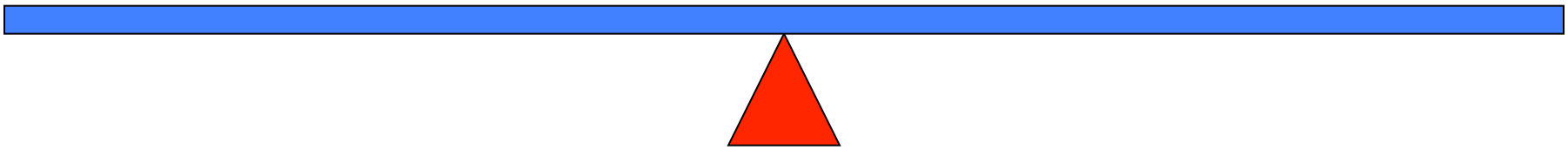
Common Features

- rules on collection, storage and utilization of health information
- roles and responsibilities of stakeholders
- scope and limit of health information privacy
- safeguards to maintain health information privacy

Striking a Balance

Information Must be Accessible to Provide Appropriate Care

Information Must be Protected to Prevent Harm to the Patient



The most secure systems are also the most useless (e.g. releasing only national-level data is more secure than releasing local data).

Cost of implementation must be weighed against the both the likelihood of harm and the severity of harm.

Continuous vigilance is required to ensure an appropriate balance between the mission of public health, which is to serve the population's health, and its ethical obligations to serve the community and safeguard privacy.

"Once basic, uniform rights in health care are established, we can return to the urgent task of providing access to health care for all... **It seems correct to view universal access to decent health care as our primary goal. But rights in health care are critical, since without them citizens may wind up with access to a system that is indifferent to both their suffering and their rights.** *"*

George J. Annas

American Bioethics: Crossing Human Rights and Health Law Boundaries.

Thank you.
Maraming salamat.

Al Alegre
alalegre@yahoo.com
al.alegre@icto.dost.gov.ph
F: /alalegre
T: @alalegre