



EMR: Electronic Medical Records Security: International Law Review

HCCA 11th Annual Compliance Institute, April 2007
Jill Nelson, RN, MBA, JD, CPC, CHC
Cleveland Clinic, Director of Corporate Compliance & Privacy Official

Electronic Medical Record Security

- E-train technology: keeping the train on the tracks
- Doing e-commerce throughout the world: some international law review
- Establishment of safety and connectivity (interoperability) standards

E-Train

- National imperative:
 - Portability
 - Interoperability
 - Quality initiatives
- Each solution creates the next problem:
 - Fear of “open” records
 - Misuse of information
 - Theft of information
 - Unauthorized access
 - Unauthorized use

E-train

- Societal benefits/hazards
 - DNA database: genetic “profiling” (insurance risk)
 - Medical error identification
 - NPI treatment patterns
 - Governmental proposals: Medicare/Medicaid computerized data
 - Research potential
- Constitutional balance
 - 4th Amendment: search & seizure—privacy “right”
 - Terrorists’ grocery
- Trend to off-shore

E-train

- Need for shared information:
 - Health care practitioner (NPI emergence of trends)
 - Patient (MyChart)
 - Transcriptionist
 - Lab
 - Radiology
 - Pharmacy
 - Coding
 - Billing (payors, governmental programs)
 - Referring physician
 - Consulting physician

International

- Canada
 - Personal Information Protection and Electronic Documents Act (PIPEDA)
 - Mandated parliamentary review every 5 years
 - Over 5 years, federal privacy commissioner has released over 350 findings in response to complaints
 - Identity theft has emerged as major criminal activity, spam, phishing
 - Even federal privacy commissioner has found herself victimized by “pretexters” who use impersonation techniques to capture personal information

Canada

- 4 Major changes (proposed)²
 - 1. Law should include a mandatory security breach disclosure requirement *for individuals whose personal information has been placed at risk*. (Many US states have such legislation).
 - 2. Law should be amended to provide the federal privacy commissioner with order-making power. Presently, this is non-binding—entitled to take the case to federal court. (HIPAA has no private right of action.)
 - 3. Presently, Canadian organizations have benefits of anonymity, even when they violate the law.
 - 4. Outsourcing of Canadians' personal information to USA makes it subject of USA Patriot Act.

UNCITRAL Model Law

- UNCITRAL (United Nations Commission on International Trade Law) adopted in 1996 as a model law
- Purpose was to offer national legislators a set of International Acceptable Rules
- Model Law details how more secure legal environment may be created for electronic commerce
- Proposed to achieve the principal of functional equivalence

India

- **Cyber Law³**

- Generic term
- Includes all legal and regulatory aspects of Internet, and all or any legal aspect or issue concerning activity in Cyber Space
- India's codified Cyber law is the Information Technology Act, 2000 (Act 21 of 2000)
- IT Act—13 chapters with 94 sections and 4 schedules
- Provides for legalized electronic commerce
- Legal recognition of electronic documents
- Admissibility of electronic data/evidence in court
- Legal acceptance of digital signatures
- Punishment for Cyber obscenity and crimes

India

Criminal Offences

Tampering with computer source documents

Hacking

Electronic forgery (false digital signature, making false electronic record)

Electronic forgery for the purpose “of cheating”

Electronic forgery for the purpose of “harming reputation”

India

- Act's shortcomings³
 - Does not cover protection of domain names
 - No provisions of enforceability on how orders need to be executed, jurisdiction of courts
 - Juvenile offences not addressed
 - No methodology of computer forensics
 - Does not cover on-line privacy, trademark and copyright
 - Does not address on-line encroachment—enabling and disabling of cookies by the individual in the browser
 - Does not address “stamp duty” aspects of electronic contracts

European Union

- Framework for data protection: numerous directives
 - Directive on Privacy and Electronic Communications⁴
 - Telecommunications, faxes, e-mail, Internet, etc.
 - Distance Selling⁵
 - E-Commerce Directives⁶
 - EU Electronic Signatures Directive⁷
 - Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Directive)⁸
- Intent to harmonize by setting fundamental guidelines for European data protection

United States

- No “right” to privacy in Constitution
 - 1st Amendment: guards speech, and private right to speak anonymously
 - 3rd Amendment: protects the home—no soldiers
 - 4th Amendment: protects against search & seizure
- Torts
 - Intrusion into private affairs, seclusion or solitude
 - Public disclosure of embarrassing private facts
 - Publicity putting person in “false light”
 - Appropriation of person’s name or likeness

United States

- Children’s Online Privacy Protection Act (COPPA) restricted collection of personal data from children⁹
- Gramm-Leach-Bliley Act (GLB) required financial institutions to disclose privacy policies & practices¹⁰
- Health Insurance Portability and Accountability Act¹¹ (HIPAA) protects privacy of medical records
 - Privacy
 - Transactions and code sets
 - Security

Other Nations Emerge

- China
- Taiwan
- Ireland
- Japan
- Russia

Safety and Connectivity (Interoperability)

- Telemedicine
- Corporate liability
- People and machines
 - Overcoming intent to commit fraud
 - Active monitoring
 - Scanning devices
 - Updating virus protection
 - Quarantines
 - Remote access
 - Singularity

Interoperability

- Interoperability:
- ability “to communicate and exchange data accurately, effectively, securely, and consistently
- With different information technology systems, software applications, and networks, in various settings
- Exchange data such that the clinical or operational purpose and meaning of the data are preserved and unaltered
- By Certification Commission for Healthcare Information Technology (CCHIT) criteria

Interoperability

- Stark selection of recipients:
- Not based on volume/value of referrals or other business
- Permitted recipient criteria include:
 - Number of prescriptions written
 - Size of medical practice
 - Total number of practice hours
 - Extent of use of automated technology
 - Membership on the donor’s medical staff
 - Level of uncompensated care

Interoperability

- Other requirements:
- Written agreement, list items and services, costs
- No restriction on ability to use the qualifying technology for any patient
- Recipient may not make receipt of the qualifying technology a condition of doing business with the donor
- Donor may not take any actions that would limit or restrict the use, compatibility, or interoperability with other systems

References

- 1 PIPEDA (Personal Information Protection and Electronic Documents Act) Dept. of Justice Canada. <http://laws.justice.gc.ca/en/P-8.6/258031.html> Last visited Dec. 18, 2006.
- 2 “Hearings Offer Chance to Fix Holes in Privacy Law.” Monday, Nov. 20, 2006. <http://michaelgeist.ca/content/view/1538/159/> Last visited Dec. 7, 2006
- 3. Information Technology Act, 2000. A. Ram Kumar, Advocate. High Court—Andhra Pradesh. Intellectual Property Rights & Information Technology.

References

- 4. Council Directive 2002/58, Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC).
http://europa.eu.int/eur-lex/pri/en/ob/dat/2002/1_201/1_2012002073/en00370047.pdf.
From article Olena Dymtredo, Cara D. Cutler. "Article: Does Ukraine Need a Comprehensive Statute to "Control" Private Data Controllers?" 5 Wash. U. Global Stud. L. Rev. 31, 2006.
- 5. Council Directive 97/7, Directive on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) (EC),
http://europa.eu.int/comm/consumers/policy/developments/dis_sell/dist01_en.pdf.
- 6. Council Directive 2001/31, Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market, 2000 O.J. (L 178) (EC), <http://europa.eu.int/eur-lex/pri/em/oj/dat/2000>

References

- 7. Council Directive 1999/93, Directive on a Community Framework for Electronic Signatures, 1999 O.J. (L#) 12 (EC). <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/1.013/1.013200001>
- 8. Council Directive 95/146, Directive on the Protection of Individuals with Regent to the Processing of Personal Data and on the Free Movement of Such Data 1995 O.J. (L281) 31.
- 9. Children's Online Privacy Protection Act, 15 U.S.C. 650 et. Seq. (1998)

References

- 10. Gramm-Leach-Bliley Act. 15 U.S.C. 6801, et seq. (1999)
- 11. Health Insurance Portability and Accountability Act (HIPAA) 42 U.S.C. 300gg and 29 U.S.C.

Questions?

- Jill Nelson, RN, MBA, JD
- Cleveland Clinic, Director of Corporate Compliance and Privacy Official
- nelsonj1@clevelandclinic.org