Privacy Guidelines for Telemedicine Developers

Peter J. Carew & Larry Stapleton

ISOL Research Centre, Waterford Institute of Technology, Ireland.

Med-e-Tel 2005, Luxemburg

Contents

- Overview of international privacy policies, practices and standards.
- The ethical position of privacy in the information society.
- Privacy framework for information systems development. [1]
- Privacy analysis of healthcare informatics. [2]
- 12 guidelines for telemedicine developers.

Privacy Milestones

- Milestones that have influenced privacy policy, thinking and legislation internationally:
  - 1948: UN Universal Declaration of Human Rights
  - 1970: Hesse, Germany. First data protection law in world.
  - 1973: US Dept of Health, Education and Welfare Code of Fair Information Practices
  - 1980: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  - 1981: Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  - 1995: EU Data Protection Directive 95/46/EC
  - 1998/1999/2000: FTC Privacy Reports to Congress
  - 2000: Charter of Fundamental Rights of the European Union
  - 2001: USA Patriot Act. Draconian anti-privacy legislation.
- The list is not exhaustive, and focuses largely on EU and US privacy developments.
- Many other countries have also passed national privacy legislation. [3]

International Privacy Practice

- Human Rights Charters. [4, 12, 13, 14, 15]
- Fair Information Practices (FIPs). [5, 6, 16, 17]
  - (1) Notice (2) Choice (3) Access (4) Security
- Council of Europe Convention. [3, 18]
- OECD Guidelines. [5, 7, 19]
  - (1) Collection limitation (2) Data quality (3) Purpose specification
  - (4) Use limitation (5) Security safeguards (6) Openness
  - (7) Individual participation (8) Accountability.
- EU Directive. [3, 8, 9, 20]
- Legislation vs. Self-Regulation. [3, 9, 10]
- International Privacy Standards. [8, 11, 21]

Privacy and Ethics

- Broadly, the ethical arguments for and against privacy can be summed up as:

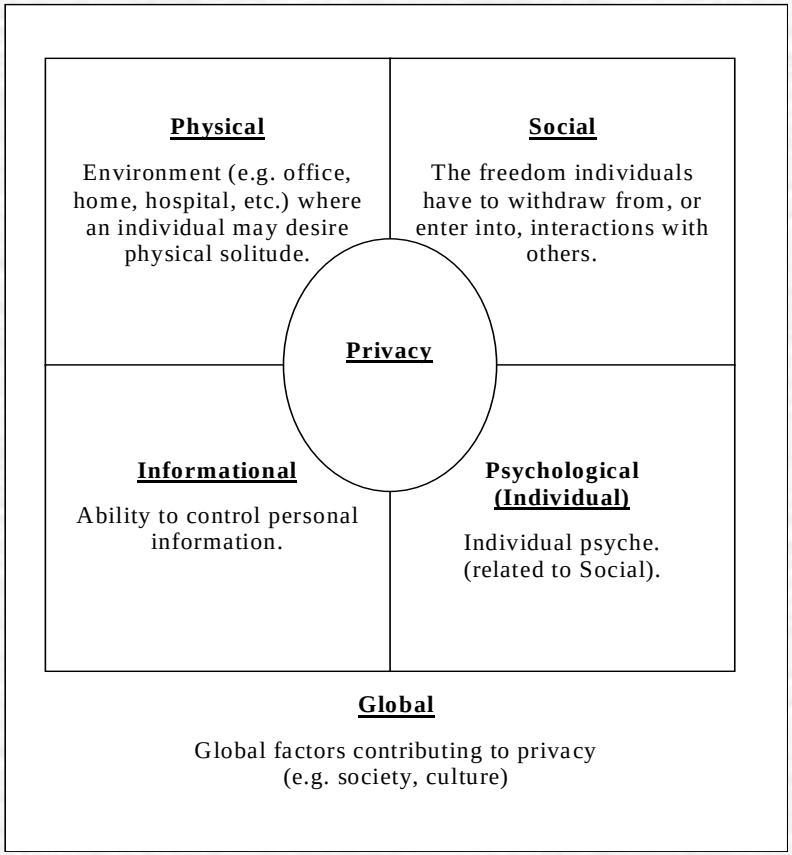
	For Privacy	Against Privacy
Privacy Perspective	Human Rights	Communitarian
Normative Ethics Category	Deontological	Utilitarian / Consequentialist

- There are arguments for both sides!
- Which ethical position is stronger remains an open question.

Privacy Guidelines for Telemedicine

- There are many generic privacy guidelines and perspectives.
- The guidelines presented here are based on an amalgamation of:
  - A recent ISD privacy framework. [1]
  - A recent privacy analysis of healthcare informatics. [2]
  - OECD Guidelines.

Privacy Framework [1]



Dimension/Id	Factor	Class
Physical		
P1	Environment	T
P2	Territoriality (Property)	T
P3	Territoriality (Body)	T
P4	Solitude (Physical)	T
P5	Repose	T
P6	Physical Access	C
P7	Sensory and Comms Channels	C
P8	Violator (Relationship)	C
Social		
S1	Intimacy (External)	T
S2	Intimacy (Internal)	T
S3	Territoriality (Status)	T
S4	Solitude (Social)	T
S5	Anonymity	T
S6	Autonomy	T
S7	Interactions and Comms	C
S8	Units	C
S9	Formality	C
S10	Personalness of Topic	C
Psychological (Functions)		
Y1	Self-Identity	F
Y2	Personal Growth	F
Y3	Autonomy	F
Y4	Contemplation	F
Y5	Self-Protection	F
Y6	Confiding	F
Y7	Emotional Release	F
Y8	Rejuvenation	F
Y9	Creativity	F
Informational		
I1	Territoriality (Knowledge)	T
I2	Reserve	T
I3	Release of Personal Info	C
I4	Distribution of Personal Info	C
I5	Use of Personal Info	C
Global		
G1	Control	C
G2	Personal Chars and Circumstance	C
G3	Organisational	C
G4	Cultural	C
G5	Societal	C

Privacy Analysis of Healthcare Informatics

- The main findings of the analysis for patients and healthcare workers (the 2 main privacy stakeholders) identified in [2] are:

	Patients	**Healthcare Workers**
Major Privacy Themes	Safety Empowerment Confiding Third Party Data Use	Territoriality Sentience & Embodiment Social Issues Autonomy

Analysis Method

- OECD Guidelines on Y axis. Privacy framework dimensions on X axis.
- Individual guidelines are considered for each dimension.
  - Dimension factors identified as relevant.
  - Privacy themes are also included as appropriate.
- A set of generic guidelines are established to mitigate privacy risks.

Analysis Results

	Physical	Social	Psychological	Informational	Global	Guideline
Collection Limitation and Consent	P7	S5	Y3, Y4, Empowerment	I3	G1, G2, G3	1 2 3
Data Quality	Disembodiment, Safety	S7, S10, Social Issues (Empathy)	Y6, Confiding	I1, I2, I3	-	4
Purpose Specification	P5	S3	Y3, Y5, Empowerment	I1, I4, I5	G1	5 2
Use Limitation	P2, P3	S1, S2, S5	Y7	I5, Third Party Use	G3	6
Security Safeguards	Safety	S5, S6	Y5	I4	G3	7 8
Openness	P8	S2, S7	Y1	I1, I4, I5	G3	9
Individual Participation	P1, P2, P3, P7	S3, S7, S6, Empowerment	Y3, Empowerment	I1, I2, I3, I4, I5, Empowerment (Access & Control of Data)	G2, G4	6 2 10 11
Accountability	P1, Disembodiment (Risk)	S3, S9	Y3, Y5	I4, I5	G5	7 12

Guidelines

1. **Limit Collection.** Only collect what is relevant and required. Unethical to gather superfluous data without careful analysis.
2. **Consent Management Facility.** Allow patients to change consent associated with individual data stored on them via some convenient interface (e.g. Web based). All consents should be "opt out" by default, as patients should explicitly authorise specific uses. Consent should be revocable at any time. Beware of coercion vs. consent.
3. **Patient Information and Training Facility.** Develop easily accessible tutorials, etc. so patients understand how data is collected (sensors), types of data collected (e.g. video, vital signs) and how it is used (e.g. in treatment, third party). Necessary for informed consent.
4. **Improved Sensors to Improve Realism in Telemedicine.** Disembodiment in telemedicine applications can be somewhat addressed in this way.
5. **Purpose Specification.** Specify purpose of all data collected at collection time (e.g. any third party use).
6. **Use Limitation.** No use beyond that specified and consented to (e.g. third party access, data mining). Data destroyed after use where possible.

...continued

7. **Security Principle.** Data stored should be kept secure from unauthorised access. Access on "need to know" basis only.
8. **Anonymity.** Patient anonymity should be supported as desired (e.g. verification vs. identification). Patient's identifying information could be stored separate from the medical data.
9. **Support Patient Data Access.** Patients should be able to easily access their data and see what uses it is being put to. Transparency.
10. **Control Principle.** Patients should remain in control of their own data and treatment wherever possible.
11. **Individuality Principle.** Different people have differing attitudes to privacy based on their personality, culture, etc. which must be supported.
12. **Professional Responsibility.** All involved in telemedicine development must take responsibility for privacy issues. It is unacceptable for engineers to dismiss privacy as a managerial issue.

Conclusions

- There are a plethora of privacy guidelines and conventions.
- No dedicated international privacy standard exists.
- The right to privacy has a predominantly deontological ethics value position.
- Privacy has many dimensions: physical, social, psychological, informational, global. All must be considered when developing information systems.
- Different stakeholders have differing privacy value positions.
- 12 general guidelines for telemedicine developers are provided.

Q&A

Contacts:
Peter Carew pcarew@wit.ie
Larry Stapleton lstapleton@wit.ie

References

- [1] Carew, P.J. and L. Stapleton (2004). Towards a privacy framework for information systems development, *Proceedings of the 13th international conference on information systems development ISD'2004, Vilnius.*
- [2] Carew, P.J. and L. Stapleton (2005). Privacy, patients and healthcare workers: a critical analysis of large scale, integrated manufacturing information systems reapplied in health, *Proceedings of the 16th IFAC World Congress, Prague, forthcoming.*
- [3] Henderson, S.C. and C.A. Snyder (1999). Personal information privacy: implications for MIS managers. *Information & Management,* **36(4)**, 213-220.
- [4] Manny, C.H. (2003). Personal privacy – transatlantic perspectives European and American privacy: commerce, rights and justice – part 1. *Computer Law & Security Report*, **19(1)**, 4-10.
- [5] Gellman, R. (2002). Perspectives on privacy and terrorism: all is not lost - yet. *Government Information Quarterly*, **19(3)**, 255-264.
- [6] Strauss, J. and K.S. Rogerson (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics*, **19(2)**, 173-192.
- [7] Ashley, P., C. Powers and M. Schunter (2002). From privacy promises to privacy management: a new approach for enforcing privacy throughout an enterprise, *Proceedings of the 2002 workshop on New security paradigms, Virginia Beach, Virginia*, 43-50
- [8] Bennett, C.J. (2000). An international standard for privacy protection: objections to the objections, *Proceedings of the tenth conference on computers, freedom and privacy, Toronto*, 33-38
- [9] Muenchinger, N.E. (2001). Information Privacy Regulation: The EU Model and the French Model. *Computer Law & Security Report*, **17(6)**, 390-394.
- [10] Steinke, G. (2002). Data privacy approaches from US and EU perspectives. *Telematics and Informatics*, **19(2)**, 193-200.

...continued

- [11] Bennett, C.J. (1997). Arguments for the standardization of privacy protection policy: Canadian initiatives and American and international responses. *Government Information Quarterly*, **14(4)**, 351-362.
- [12] 1948: United Nations Universal Declaration of Human Rights (Article 12)
- [13] 1950: Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8)
- [14] 1966: International Covenant on Civil and Political Rights (Article 17) (in force 1976)
- [15] 2000: Charter of Fundamental Rights of the European Union (Article 8)
- [16] 1973: “Records, Computers, and the Rights of Citizens”, US Dept of Health, Education, and Welfare Report
- [17] 1998: “Privacy Online: A Report to Congress”, FTC Report to Congress
- [18] 1981: Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- [19] 1980: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- [20] 1995: EU Data Protection Directive 95/46/EC
- [21] 1996: Canadian CSA Model Code for the Protection of Personal Information