



Governance and Data Protection in the Health Sector

Billy Hawkes

Data Protection Commissioner

State Claims Agency

Clinical Indemnity Scheme Seminar

Farmleigh, 27 October 2011

Presentation Outline

- What Should Be
- What Is
- What Can Be?

The Governance Challenge

- What does an Organisation in the Health Sector need to do to be considered a good “corporate citizen” in its treatment of personal data?
- How would it demonstrate this accountability in practice:
 - *To its Customers/Clients?*
 - *To a Regulator?*

Accountability: Essential Elements

1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies into effect, including tools, training and education.
3. Systems for internal, ongoing oversight and assurance reviews and external verification.
4. Transparency and mechanisms for individual participation.
5. Means for remediation and external enforcement.

http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

Demonstrating Accountability

- Policies
- Executive oversight
- Staffing and delegation
- Education and awareness
- Ongoing risk assessment and mitigation
- Program risk assessment oversight and validation
- Event management and complaint handling
- Internal enforcement
- Redress

Data Protection – a Fundamental Human Right

- *Implicit* Right to Personal Privacy under Irish Constitution – Article 40.3.1
- *Explicit* Right to Personal Privacy under Article 8 of 1950 *European Convention for the Protection of Human Rights & Fundamental Freedoms* [ECHR]
 - *ECHR now indirectly part of Irish law due to ECHR Act 2003*
- *Explicit* Right to Data Protection under EU Treaties – Lisbon Treaty and EU Charter



EU Charter of Fundamental Rights: Article 8

- **Protection of personal data**
- *1. Everyone has the right to the protection of personal data concerning him or her.*
- *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
- *3. Compliance with these rules shall be subject to control by an independent authority.*



EU & Irish Legislation

- Data Protection Directive 95/46/EC
 - *Being updated*
- Data Protection Acts 1988 & 2003
- Electronic Privacy Directive 2002/58/EC (as amended by 2006/24/EC + 2009/136/EC)
- EC Electronic Privacy Regulations 2011 (SI 336/2011)

Data Protection & Health Data

- Data on *physical or mental health or condition or sexual life* are '**sensitive personal data**' with special protection
- Complements ethical duty of medical confidentiality

Eurobarometer Survey (2011): Privacy most important in relation to:

1. Medical Records
2. Financial History
3. Credit Card Details
4. PPS Number
5. Garda Record
6. Social Welfare History
7. Telephone / Internet Records
8. Personal Emails
9. CV Details
10. Personal Telephone Number

Presentation Outline

- What Should Be
- **What Is**
- What Can Be?

Health Sector Audits: 2007-1010

- Large Public Hospital
- Large Voluntary Hospital
- 5 GP/General Clinics
- Health Insurer
- Nursing Home Repayment Scheme
- Pharmacy
- Out-of-hours Facility

Large Voluntary Hospital Audit

- *"good organisational awareness of data protection principles"*
- *"good technical security measures were in place"*
- Main concern: physical security
 - *Access to Chart Room*
- Positive response to specific recommendations

Large Public Hospital Audit (1)

- *“Data protection, from a governance perspective, is falling well short of what would be expected in an organisation collecting and processing vast amounts of sensitive personal data”*
- *“Critically, it is unclear where responsibility lies for the practical application of data protection policies and procedures on a day to day basis ... In order to correct the many data protection concerns which have been highlighted in the report, this issue of responsibility must first be addressed.”*
- *“Having regard to the primary goal of the audit “to establish whether care was delivered in a manner that gave due respect to the legitimate privacy expectations of patients”, the issues raised in this audit are of such a scale that this Office is not in a position at present to indicate that this is the case.”*

Large Public Hospital Audit (2)

- *" In terms of security alone, the inspection Team encountered numerous breaches of the Data Protection Acts during the course of the audit, including:*
 - *Files left in public / unsecure areas*
 - *Inoperative security mechanisms on file storage areas*
 - *Patient data stored in corridors*
 - *Medical data sent by unsecure email*
 - *USB ports not locked down*
 - *Lack of system access controls*
 - *Lack of physical access controls to sensitive areas"*

GP Clinics

- *"good awareness of data protection principles generally"* .
- *"one area requiring attention is the location and storage of the physical patient files"*
- IT Security
- Extent of access to medical records by non-medical personnel
- Data Retention

Follow-up: GPs

- *“A Working Group was established in early 2010 following the discussions between the Office of the Data Protection Commissioner and the ICGP in response to the findings of the Office of the Data Protection Commissioner following audits it carried out on a number of GP practices”*
 - *Foreword to [A Guide to Data Protection Legislation for Irish General Practice](#), April 2011*
- *Guide, Templates @:*
http://www.icgp.ie/go/in_the_practice/information_technology/data_protection

Follow-up: Hospitals/General

- Input to HIQA work on *Standards for Health Information Governance*
 - <http://www.hiqa.ie/standards/health-information-standards>
- Input to *Health Information Bill*

Presentation Outline

- What Should Be
- What Is
- **What Can Be?**

Good Practice: General

- *Transparent* and *Balanced* approach to collecting and using patient data
- Patients should know what you are doing with their personal data
- Consult DPC and other guidance (www.dataprotection.ie)

Good Practice: Audit

- Do we know what types of personal data we hold?
 - *Electronically (also CCTV images)*
 - *Paper*
- Can we justify:
 - *Why we collect it?*
 - *What it is used for?*
 - *Length of time we hold it?*
 - *Who has access to it?*
 - *Who it is disclosed to?*

Good Practice: Access & Correction Requests

- Can we :
 - *Provide a description of the personal data we hold on an individual patient within a max. of 20 days?*
 - *Provide copy of this data within a max. of 40 Days?*
 - *Correct or erase data within 40 days?*

Good Practice: Security

- Access Controls
 - *Electronic patient systems secure*
 - *Paper Files*
 - *Audit Trails*
- Vulnerabilities
 - *Portable Devices*

Good Practice - Need to Know Access

- Must be able to stand over all access to personal data as justifiable within an organisation
 - *Balance between needed access and data protection*
- ECHR Judgment of 17 July 2008 - CASE OF I v. FINLAND (Application no. 20511/03) – obligation to be able to stand over all access to health data on a need to know basis
- Access to sensitive personal data must be even more restricted. Locked cabinets for manual data etc
- Different medical teams/different users – different access

Good Practice: Disposal

- Do not retain patient records for any longer than can be *objectively* justified: clear policy
- Comply with legal retention obligations
- **Orderly** and **secure** disposal of old records

Good Practice : People

- Does everyone handling personal data know their responsibilities under Data Protection Law? Is this routinely included in training/induction?
- Are procedures for handling personal data properly documented?
- Are DP compliance responsibilities clearly allocated?

Good Practice: If things go wrong ...

- Have a clear plan – what will you do if there is a security breach?
- Notify DPC and patients
 - *DPC Code of Practice and Guidance*
- Tell patients how you intend to remedy any damage done to their interests

Good Practice - Research

- Anticipate how you intend to use patient data, fully inform patient and get **written consent** *or*
- **Anonymise** the data *effectively* (DP legislation only applies to data attributable to an *identifiable* person) before using for research – still best to tell the patient
- Consult DPC Guidelines
 - *Data Protection Guidelines on Research in the Health Sector*
 - http://www.dataprotection.ie/documents/guidance/Health_research.pdf

Thank You

Office of the Data Protection Commissioner
Canal House
Station Road
Portarlinton
Co Laois

Phone: LoCall 1890 252231
057 8684800

Fax: 057 8684757

Email: info@dataprotection.ie

Website: www.dataprotection.ie