

Data Protection

Mobile Health, Telemedicine and Patient Confidentiality

Jim Gregg

Professional Development Consultant
Irish Computer Society

1st April, 2016



Business Analysts Association of Ireland



itsSMF.ie
The IT Service Management Forum

Professional Training



TECH WEEK

ICS GRID



Computing Curriculum



Healthcare Informatics Society of Ireland
~Cumann Ríomheolais Sláinte~
Incorporating the Healthcare Informatics sections of the Royal Academy of Medicine in Ireland and of the Irish Computer Society

dpo.ie

the association of data protection officers



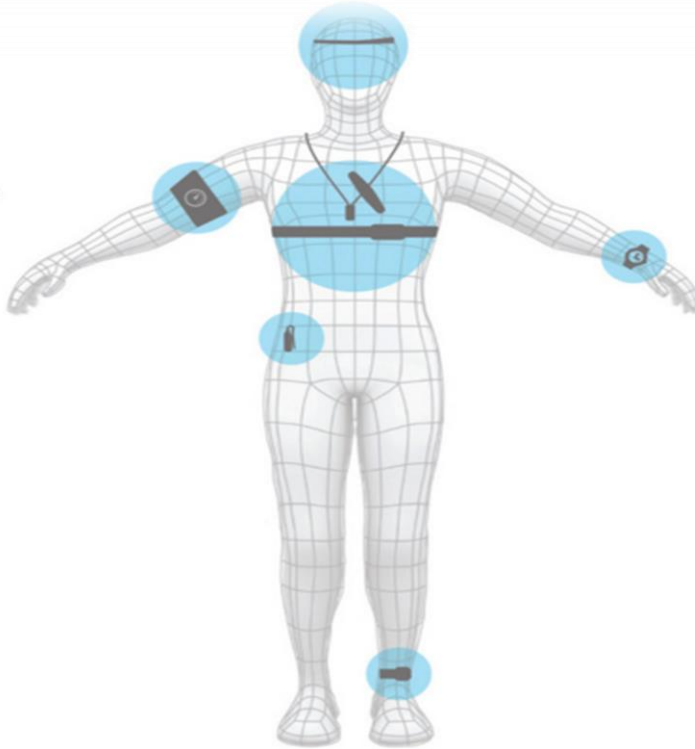
Technology, Connectivity & Health








Technology & The Connected Landscape

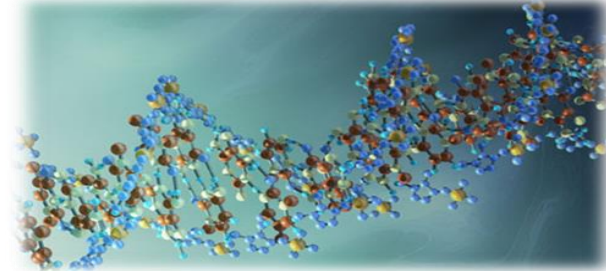
- In 2016, the internet currently has over 4.63 billion pages
- There will be nearly 18.9 billion network connections (Cisco)
- 6.4 Billion Connected "Things" Will Be in Use in 2016 (Gartner)
- IOT will triple to “38 billion” devices by 2020 (Juniper Research)

The Connected Landscape & Health Monitoring

-  **Posture**
Lumo
Zephyr
Jins Meme
-  **Muscle Activity**
Athos
-  **Blood Pressure**
iHealth
Withings
-  **Skin Conductance**
Basis
BodyMedia
Empatica
Neumitra
-  **Movement**
Fitbit
Nike Fuelband
Jawbone Up Band
Garmin
Samsung
MC10
Zephyr
Withings
Spire
iHealth
Jins Meme
Proteus
Neumitra
BodyMedia
Empatica
Owlet
-  **Oxygen Level**
iHealth
Withings
Owlet
-  **Hydration**
Corventis
MC10
-  **Temperature**
Tempdrop
MC10
Empatica
BodyMedia
Basis
Owlet



-  **Brain Activity**
NeuroSky
Melon (acquired by DAQRI)
Emotiv
-  **Glucose**
Google
Dexcom
Glysens Incorporated
-  **Eye Tracking**
Jins Meme
-  **Sleep**
Fitbit
Rest Devices
Garmin
Nike
Amigo
BodyMedia
Withings
Samsung
Misfit
Jawbone
iHealth
Basis
Owlet
-  **Respiration**
Spire
Zephyr
Rest Devices
-  **Ingestion**
Proteus
-  **Heart Tracking**
Zephyr
Withings
Sprouting
Proteus
iHealth
Basis
Corventis
AliveCor
Samsung
Garmin
Empatica
Owlet



* This is not a comprehensive list

SanTech

Let's start with the Legislation

Legislation

Data Protection Act 1988 and Amendment Act 2003

EC Privacy and Electronic Communication Regulations 2011

New EU General Data Protection Regulations 2016

Definition of Processing

Processing

Performing any operation or set of operations on data, including:

- obtaining, recording or keeping data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or data by transmitting, disseminating or otherwise making it available,
- aligning, combining, blocking, erasing or destroying the data.

The 8 Rules of Data Protection (Current Legislation)

These are the 8 Principles of Data Protection

1. Fairly obtained and processed
2. Specified & lawful purpose
3. Not incompatible with purpose or purposes
4. Safe and secure
5. Accurate & up-to-date
6. Adequate, relevant & not excessive
7. Not retained for longer than is necessary
8. Subject rights of access

The Changing Landscape of Data Protection

Some new kids in town...

In the last 12 months in the ODPC.....

- Budget has trebled (new premises in Dublin)
- Staff headcount has doubled
- Compliance audits more focused (sectoral expertise)
- Language is more aggressive
- Health sector name checked

New EU General Data Protection Regulations 2016

- Far greater scope - 90 Provisions (Current Legislation = 36)
- Increased fines (Up to 5% Global Turnover)
- Dedicated DPO (Public Bodies)
- Explicit Consent (not implied/presumed)
- DPC can issue fines directly

Specific to this conversation....

- Special Categories of Data (Replaces Sensitive Personal Data)
- Privacy By Design & Default
- Privacy Impact Assessment
- Profiling

All Now Statutory Obligations

Special Categories of Data

- It replaces the term 'Sensitive Personal Data'. Scope extended to include;
 - Genetic data e.g. DNA
 - Biometric data e.g. fingerprint, retina scanning, voice recognition
 - Health Data

Privacy By Design

- Means that each new service or business process that employs usage of personal data by DC/DP must give consideration to the protection of such data as a default rule.
- DC needs to be able to show that adequate personal data security and safety measures are in place.
- No need to retrofit e.g. IT department must take privacy into account during the whole life cycle of the system or process development and implementation

Privacy By Default

Data Protection by Default simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service (WhatsApp)

- In other words, no manual change to the privacy settings should be required on the part of the user.
- There is also a temporal element to this principle
 - personal information must by default only be kept for the amount of time necessary to provide the product or service.

Privacy Impact Assessment

- If processing can potentially result in high risk to the rights and freedoms of individuals
- DCs must think before data is processed or used
- An assessment be performed before personal data is processed
 - Description of the envisaged processing operations
 - Processing purpose(s) and proportionality
 - Assessment of risks
 - Mitigation steps

Profiling

Profiling means any form of automated processing of personal data that allows evaluation of certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's;

- **health**
- performance at work & economic situation
- personal preferences & interests
- Reliability & behaviour
- location or movements

Profiling

- DS must be informed at the time data is collected that profiling will occur
- DS may also inquire of a DC and receive confirmation of any such processing, including profiling and its consequences, at any time
- DS can object to processing by profiling but not altogether,
 - Where lawful processing conditions need to be met
- DC must respect data subjects' rights regarding profiling - cease processing upon DS objection.

So, where do we start?

Here are some recommendations

- Conduct a Data Protection Audit/Executive Review
- Create Policies
- Develop Processes & Procedures
- Staff Awareness & Training

Need Help?

Jim Gregg

Professional Development Consultant
Irish Computer Society

Tel 01 644 7820

Mob 086 047 6840

Email jimgregg@ics.ie

Thank You

Jim Gregg

Professional Development Consultant
Irish Computer Society

Tel 01 644 7820

Mob 086 047 6840

Email jimgregg@ics.ie

Irish Computer Society

87-89 Pembroke Road
Dublin 4

Electronic Health & Data Protection

EHR - National Standards for Better Safer Care

- Information Governance
- Data Quality
- Privacy/Confidentiality
- Privacy Impact Assessment
- Information Security
- Primary/Secondary Use of Data
- Consent
- Statement of Information Practice

“Actively supporting and enabling a culture of patient safety and quality improvement.”

These are the 8 Principles of Data Protection

1. Fairly obtained and processed
2. Specified & lawful purpose
3. Not incompatible with purpose or purposes
4. Safe and secure
5. Accurate & up-to-date
6. Adequate, relevant & not excessive
7. Not retained for longer than is necessary
8. Subject rights of access