Recent Policy Initiatives in the EU for Data Protection for the Health Sector Based on GDPR

Contribution for Research Workshop:

Telehealth Technology, Service, and Research Trends: Perspectives from Asia, EU, US

By Erik Bohlin, Chalmers University of Technology

Research and collaboration support from Dr. Simon Forge, SCF Associates, is gratefully acknowledged

Date: Sunday, 20 January, 2019

Time: 15:30-16:45

Location: Mid-Pacific Conference Center, South Pacific 2

Health security and the EU General Data protection Regulation (GDPR) impacts

Direct impacts –

- Patients
- National health services
- E-commerce for health supplies
- Behaviour of Industry players – pharmaceuticals industry, online pharmacies, private health insurers and their related partnerships

In May 2017, the UK NHS computer systems suffered severe cyberattacks

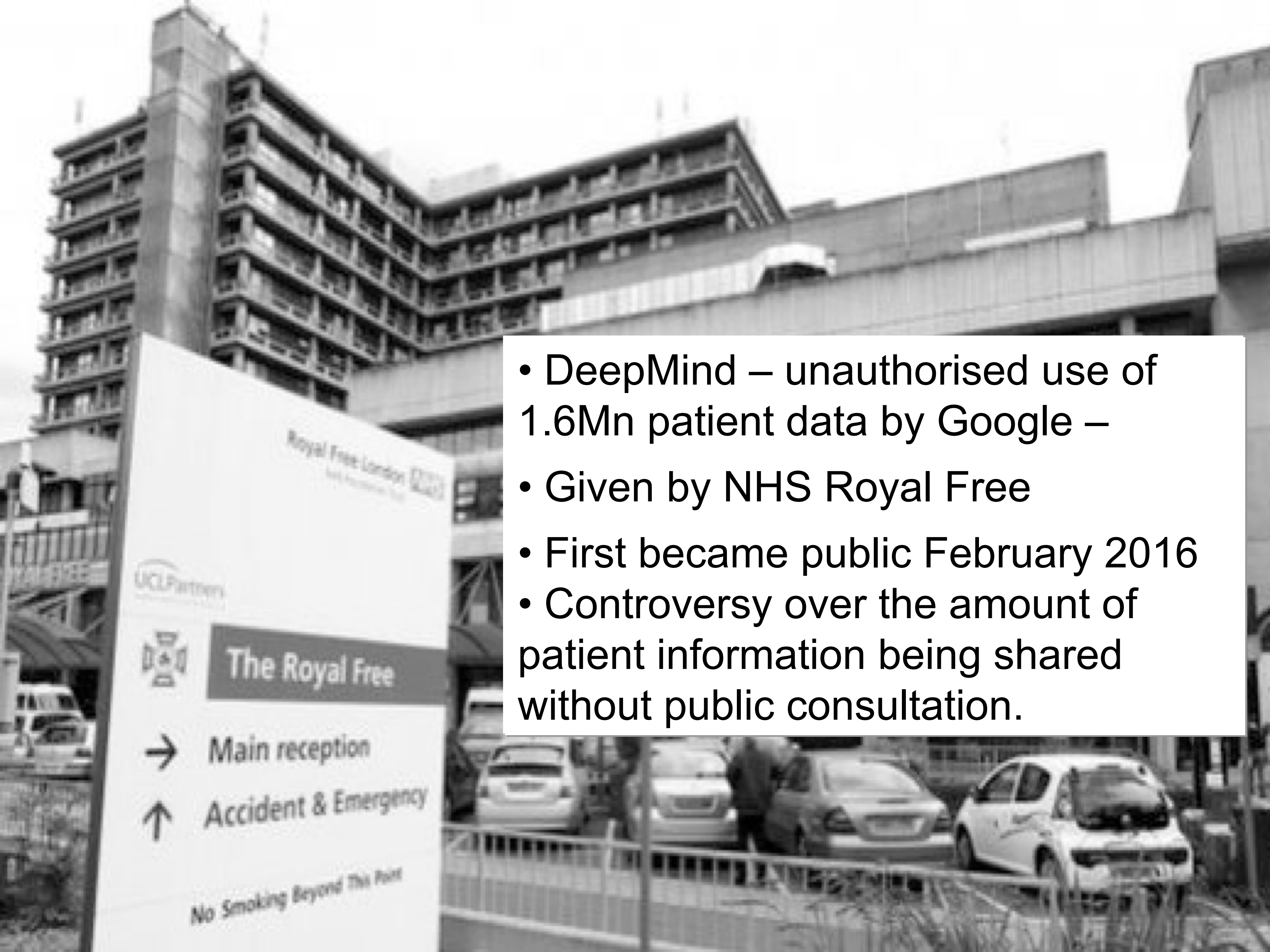
Wannacry attack from rogue states – destroys data – does not just lock it up

- Patient records stolen
- Staff locked out of systems for emergency patient treatment - ransomeware
- Staff unable to access patient monitoring and medical treatment for current care
- Management of hospitals, operating equipment, beds and staff frozen

Because no effective data protection measures in place

•Other NHS systems have suffered data breaches in the past

- Unreliable access to patient records and losses of key data
- Fragmentation of NHS patient records across hospital sites and departments as well as outpatients and GP surgeries
- Trust – NHS broke privacy laws – national – in 2017 according to the Information Commissioner's Office and that would break GDPR in 2018



- DeepMind – unauthorised use of 1.6Mn patient data by Google –
- Given by NHS Royal Free
- First became public February 2016
- Controversy over the amount of patient information being shared without public consultation.

GDPR also acts as an effective preventive measure in health related e-commerce

Threat is that the e-commerce chains will resell patient data:-

-To pharmacists and related merchants – eg heath products

-To data brokers who provide profiling of patients to marketeers, drug companies etc

-To private health insurers who wish to profile prospective customers with inside knowledge that may be confidential and private

GDPR secures patient data through 4 mandates on its use:-

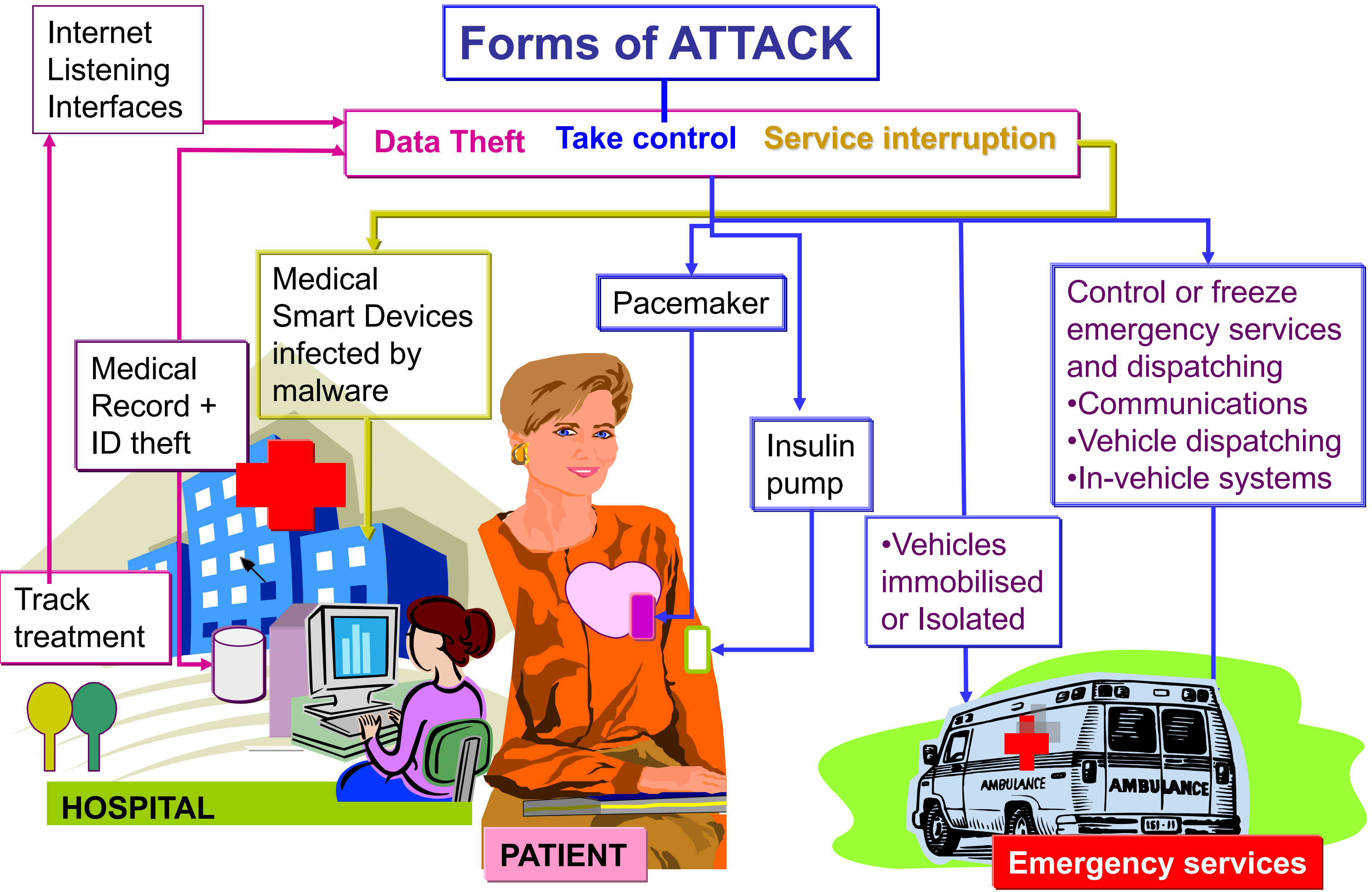
- The data is only available if an explicit opt-in permission is given by a patient
- The data can only be used for the purpose that the patient permitted
- The data cannot be passed to any third party without a further opt-in process
- Patient data is of a particular and sensitive kind and its protection must be far higher than for other personal data

Data Breaches and Cybersecurity attacks have occurred on UK NHS hospitals, especially patient record systems

11 Key NHS hospital systems require both security and privacy protection:-

- Hospital-wide communications for staff and for patient tracking
- Patient record databases, especially medical treatment history
- Accident and emergency centres, communications and equipment
- Bedside monitoring systems and treatment documentbases
- Management of nursing care and medical staff in real-time
- Pathology labs and localised pathology systems, including in-vehicles
- Operating theatre systems
- Outpatient management systems
- GP communications and the outpatient environment
- Emergency services dispatch, in-vehicle systems and staffing
- Pharmacies, pharmacy databases and logistics supply chains.

IoT attacks - not just critical infrastructure : health front attacks



GDPR provides the shielding EU Regulation on data protection for the health service data and its daily operations

1. GDPR introduces the notion of institutional protection of the data held

2. This is the key foundation of protection of health data in the EU

3. Its strong penalties put the onus of effort for protection of patient data and care processes on the health authorities

4. The UK NHS gives one of the clearest examples of its necessity – the ransomeware and other attacks which demand far greater data protection measures.

General Data Protection Regulation of privacy of the citizen

GDPR Principles:-

1. Personal data must be processed lawfully, fairly, and transparently
2. Personal data can only be collected for specified, explicit and legitimate purpose
3. Personal data must be adequate, relevant and limited to what is necessary for processing
4. Personal data must be accurate and kept up to date
5. Personal data must be kept in a form such that the data subject can be identified only so long as required for processing
6. Personal data must be processed in a manner that ensures its security
7. The owner of the data is the person – some MS go further (France)
8. The person must be aware that the data has been collected and has given consent.
9. All citizen’s have the ‘right to be forgotten’ and can withdraw permission.

The rights of patients according to GDPR,

The GDPR includes a number of rights for patients (the data subjects) with their explicit and conscious opt-in being required to use their data.

The opt-in by the patient must be given in response to an explicit and clear request from those holding data, or wishing to, with the patient's principal rights being to:-

1. **Be informed** of data and privacy rights – to be met by *provision of privacy notice*
2. **Access own data** – with a right to obtain a copy of all personal data held by NHS – the *subject access right* or **SAR**
3. **Correction** – the right to require any inaccurate data held by NHS to be rectified
4. **Erasure – RTBF** – the '**right to be forgotten**' – destruction of all personal data
5. Demand **restriction of processing** of personal data
6. **Data portability** (with the data provided in a common electronic format)
7. **Halt processing** of personal data in particular situations
8. Control over **automated decision-making** including profiling
9. **Right to complain** to the Information Commissioner's Office, and have that complaint followed through a standard process with time limits and set actions.

GDPR brings 3 specific health-related data definitions

•**1 Personal data** - relates to physical or mental health information including services provision of person

•**2 Genetic data** - personal data as is any data unique to the data subject related to inherited characteristics including facial image or scoped or probed data

•**3 Biometric data** - personal data from technical processing of personal information on physiological, physical, behavioural or mental characteristics that uniquely identify a person

PLUS - all such medical data must be held to be at a higher standard of protection than more general personal data.

GDPR requires Data protection impact assessments (DPIAs)

•Under the GDPR, “data protection impact assessments” (DPIAs) will be required when health data of any of the 3 kinds mentioned is processed on a large scale.

•A DPIA is a type of risk assessment of the impact of the anticipated processing activities on personal data

•A Data Protection Regulator will also have to be consulted prior to personal data being processed when an assessment indicates that the processing would result in a high risk in the absence of measures taken by a data controller to mitigate the risk

General Data Protection Regulation - enforcement

Key Features of its penalties:

Financial repercussions:-

•Regulation states that fines are intended to be effective, proportionate, and dissuasive

•The intent is that they should not be needed, as all data controllers (in enterprises, etc) and processors will comply:

•Negligent or Intentional infringements, or infringements that involve multiple provisions of the Regulation, will be subject to major fines of up to €20 million or 4 % of annual global turnover, whichever is the greater

•Functional, operational or administrative infringements fines of up to €10 million or 2% of annual global turnover, whichever is the greater

•In addition: The Regulation grants data subjects the rights to claim damages for *non-financial losses*, such as distress.

THANK YOU