



# EU Standards in eHEALTH covering privacy, security and ethics



C3L Scott Cadzow – [scott@cadzow.com](mailto:scott@cadzow.com)





# The foundation of (e)Health

Where we need to start from



# Our founding principles

- Whereas recognition of the **inherent dignity** and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world ...
- Whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in **the dignity and worth of the human person** and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom ...

# Our founding principles cont'd

- Article 1 of the UDHR
  - All human beings are born free and equal in **dignity** and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.
- Article 22 of the UDHR
  - Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his **dignity** and the free development of his personality



# What that means

- Effective, timely, correct, health monitoring and medical intervention that is ethical, fair, equitable and treats both the patient and the care system actors with “dignity”
- Key to much of this is understanding of the context
  - What is “right” is not a binary thing





# Standards and (e)Health

A personal (UNCAP) view



# EU standards efforts on behalf of UNCAP

- First: Why EU standards?
  - It's an objective of the H2020 programme to enable open access to all – that means open code (open reference implementation) and open standards (open reference design and requirements). EU standards are developed across the trinity of CEN/CENELEC/ETSI with ETSI having primary responsibility in ICT and direct industry support
- Second: Who are we doing EU standards with?
  - For geo-eHealth OGC feeding into CEN TC287 (GiST, Trilogis leading this effort)
  - ETSI for ICT and the eHealth landscape across core networks, cellular networks, M2M, IoT, radio devices, security, privacy, law enforcement (C3L leads this effort)

# eHealth and geo-eHealth

- Geo-eHealth tags medical events with geo location data
  - Used to identify where an event occurred
  - Assists locating source of outbreaks and measuring spread to assist in mitigation
  - Can also be used to geo-tag medical equipment for geo-discovery
  - Can be used to geo-tag patients
    - Ethics and privacy concern – addressed by developing work in privacy-by-design, privacy-by-default, secure-by-default programmes

# Recent activity at ETSI #1

- Ongoing development of ETSI Work Item DTR/eHEALTH-007, “Standardisation use cases for eHealth”
  - Scope from ETSI Work Programme Management states:
    - *“To present a number of typical use cases in the eHealth domain and from their analysis to identify gaps in standardisation. The analysis should cover aspects of link connectivity, network interconnectivity, semantic and syntactic interoperability, security (risks and provisions), and the existence of standards to meet each aspect. Furthermore the analysis should clearly identify actors and their roles, for each of primary, secondary and tertiary involvement in the use case. Examples will be sought from industry, from existing and completed FP7 and H2020 projects and from current eHealth and Health industry practices.”*
  - Scope statement in latest draft of work item presented to March 2016 meeting of ETSI EP eHEALTH:
    - *“The present document presents a number of typical use cases in the eHealth domain and their analysis to identify gaps in standardisation. The analysis covers aspects of link connectivity, network interconnectivity, semantic and syntactic interoperability, security (risks and provisions), and the existence of standards to meet each aspect. Furthermore the analysis identifies actors and their roles, for each of primary, secondary and tertiary involvement in the use case.*
    - *The use case examples have been drawn from industry, from existing and completed FP7 and H2020 projects and from current eHealth and Health industry practices ”*

# Recent activity at ETSI #2

- Panel member at ETSI “[5G: From Myth to Reality](#)” event
  - 213 attendees, placing eHealth and IoT at heart of 5G
- Contributions to ETSI EP eHEALTH Meeting
  - IoT and eHealth
  - Role of Ethics and Dignity in eHealth
  - Plus draft of work item itself



# Planning and planned activity at ETSI

- ETSI Security Week (June 2016)
  - Focus is on IoT, hoping to be on the panel for eHealth/Privacy/Ethics debate
- ETSI CYBER meeting (June 2016 ++)
  - To further develop the Identity Management thread for privacy by design – this invokes semantic identity protection and thought models for cryptographic protection in mutable many-to-many environments such as evidenced in eHealth scenarios
  - To propose work item for eHealth thread in Critical Infrastructure Protection domain
  - To address protection schemes in massively virtualised environments covering global eHealth (billions of devices, billions of affected users, hundreds of millions of health professionals) with secure/private non-centralised core
- EP eHEALTH meetings (June 2016 ++)
  - Development of core use case report and expansion of IoT work





# Security and (e)Health

The drivers to be aware of to give standards based security provisions



# The domain challenge

- Very challenging domain
  - Mutable by default
    - Patients change, health interventions change, medical professionals change
  - Unplannable by default
    - Cannot know when a patient will get ill and with what condition
  - Expectations of intervention are getting more demanding
    - Life expectancy is (generally) increasing
    - Demographics are themselves mutable:
      - Aging populations, older entry to parenthood, greater urbanisation, greater number of sedentary lifestyles, mechanisation of food production,

# The security paradigms

- Conventionally CIA
  - Confidentiality, Integrity, Availability
- Conventionally “document” based
  - Secures a “thing” against attack
- Conventionally risk centred



# Some conclusions

On standards for (e)Health



# On security of the (e)Health domain

- No one standards body can do this but ...
  - We cannot treat eHealth bit-by-bit
  - We have to do some serious work to state the problems
  - We have to recognise the mobility of all the actors and that eHealth is therefore a global and mobile problem
  - We have to recognise that whatever we do now will need to change later – the mutability of society demands that recognition
- Thus ...
  - ETSI, ISO, HL7 and all stakeholders have to come together to work on the standards aspects

# Some thoughts on funding

- The health market is worth many billions of \$/£/€ annually
- Standards in eHealth are effectively unfunded (a few tens of thousands?)
- No standards will lead to fragmentation – lots of little proprietary markets (even if little could be 100s of millions of \$/£/€)
- Invest in standards – bigger market, better healthcare



# Questions?

- Answers?

