Standardisation and Health: Under the Microscope

ETSI – Security and Dignity

Co-funded by
the Horizon 2020 Framework Programme
of the European Union

Your speaker

- Scott CADZOW
  - Director, Consultant, Security Expert, Standards developer, Pen-tester, Cryptanalyst (for fun), Writer/Blogger (not often), Husband, Father, Privacy advocate, Triathlete (barely competitive but enjoys it), Park runner
    - Polymath of standards
  - Rapporteur of about 20 ETSI standards (TETRA, NGN, HF-UCI, MTS, AT-D, ITS, eHEALTH, CYBER, LI, QSC)
  - Chairman or vice chairman at various times of ETSI and ISO standards groups (TETRA, LI, ITS)

Setting the tone

- “Real knowledge is to know the extent of one’s ignorance”, Confucius
- “... as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know”, Donald Rumsfeld (February 2002)
- “He that would perfect his work must first sharpen his tools”, Confucius

Why standards?

- Multi-vendor market growth requires standards
  - One vendor can supply what he can manufacture and support
  - One open standard allows multiple suppliers, multiple supporting organisations, greater intellectual involvement in the market
- Populations are changing and Healthcare is too
  - Increasing need to focus on long term wellness – not intervention for illness
  - Fixing problems is often expensive as problem is often chronic before intervention is sought
  - Need to integrate wellness and life-care into healthcare
  - Need to ensure choice in the wellness market and compatibility with healthcare

Role of standards

- To give assurance of semantic and syntactic interoperability
- To guide – not to prescribe – builders and developers to conform
- Clearly indicate what is mandatory and what is optional
  - Ideal standards are “tight” – few options and even where options are described their behaviour is mandated
- Designed for proof of functionality
  - Design for Test
  - Design for Assurance
  - Design for Privacy

Underlying societal issues behind UNCAP and eHealth

- Increasing realisation that health professionals are not responsible for delivering healthy populations
  - Variables in delivering a healthy population are too numerous
    - Context is everything
  - Health issues are highly volatile and mobile
    - The mobility of the population and its size are major factors
- Societal responsibility for health and well-being cannot be devolved to the health service alone
  - Individuals have to accept responsibility
  - Communities have to accept responsibility

More societal issues …

- Society is mobile … so healthcare has to be mobile too
  - Health records available anywhere? To widely recognised groups of health professionals?
    - What is a health professional?
    - Who determines that classification?
- Populations are aging
  - Health issues which were uncommon when people lived to 50 are now widespread as we expect to live to 90 or beyond
  - Healthcare for the elderly is in its infancy … and as populations age there will be an increasing gap in age between the carer and the cared

Co-funded by the Horizon 2020 Framework Programme of the European Union

Yet more societal issues …

- Humans are not identical
  - We cannot treat people as machines
  - Psychology is an important element of health
  - Support networks are inconsistent

EU view on eHealth

- eHealth is regarded by Europe's Information Society eHealth portal as
  - "today's tool for substantial productivity gains, while providing tomorrow's instrument for restructured, citizen-centred health care systems and, at the same time, respecting the diversity of Europe's multi-cultural, multi-lingual health care traditions. There are many examples of successful eHealth developments including health information networks, electronic health records, telemedicine services, wearable and portable monitoring systems, and health portals".

EU initiatives … historic?

- Mandate M/403 of the European Commission Enterprise And Industry Directorate-General: "Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies, applied to the domain of eHealth".
  - Produced ETSI TR 102 764 in 2009
  - Addressed architecture, communications modes and attributes
  - Did not address open data

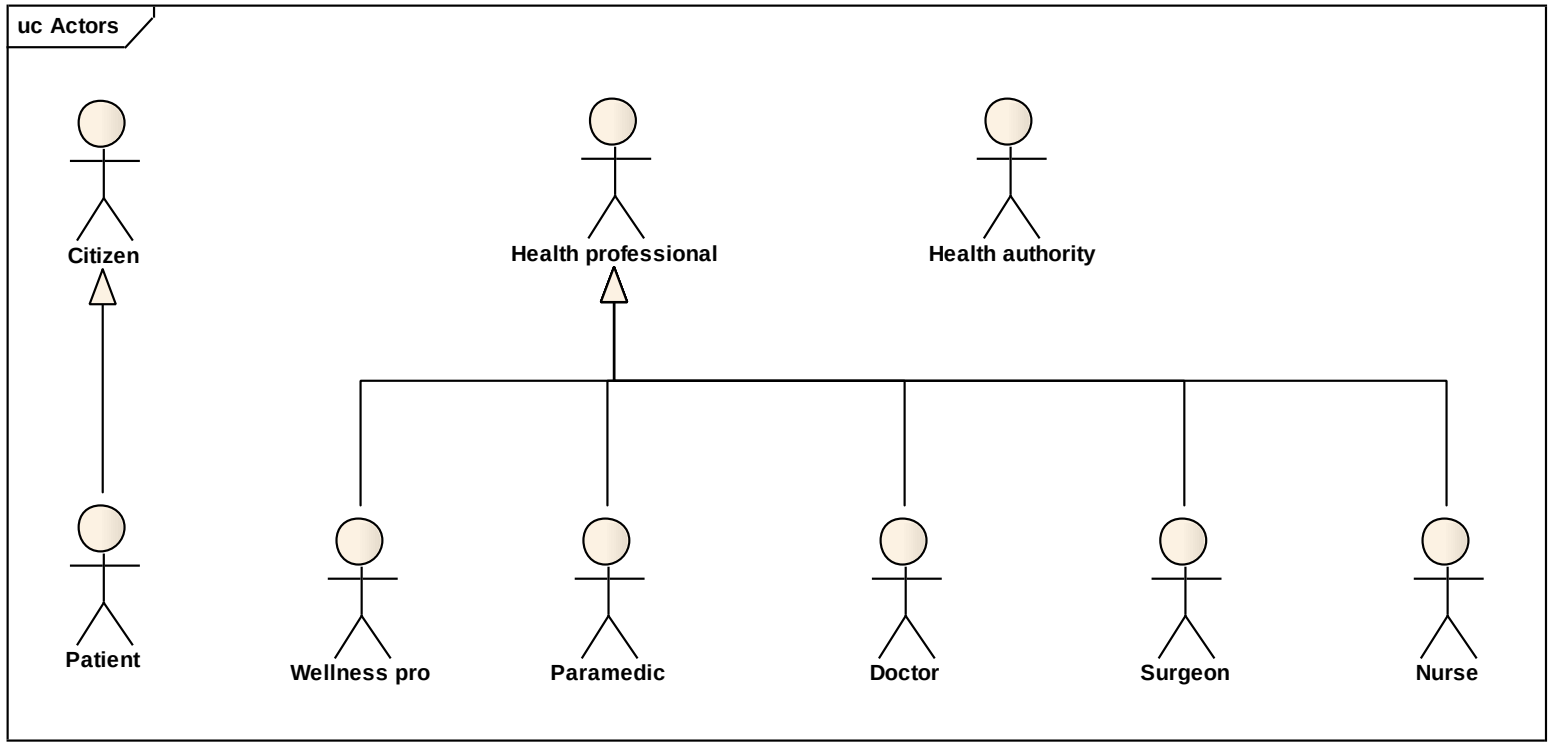
Rationale for eHEALTH

- A summary of the important overall problems regarding healthcare services that most countries are facing:
  - increased demand on healthcare resources;
  - demand for increased accessibility of care outside hospitals;
  - need for increased efficiency, individualization and equity of quality-oriented healthcare within limited financial resources;
  - difficulties of recruiting and retaining personnel in the healthcare services.
- eHealth will offer a toolkit for timely, efficient, and high quality healthcare including:
  - allowing the migration to self-managed care;
  - allowing increased patient mobility at an international level (e.g. cross border).

Ethics versus security and privacy

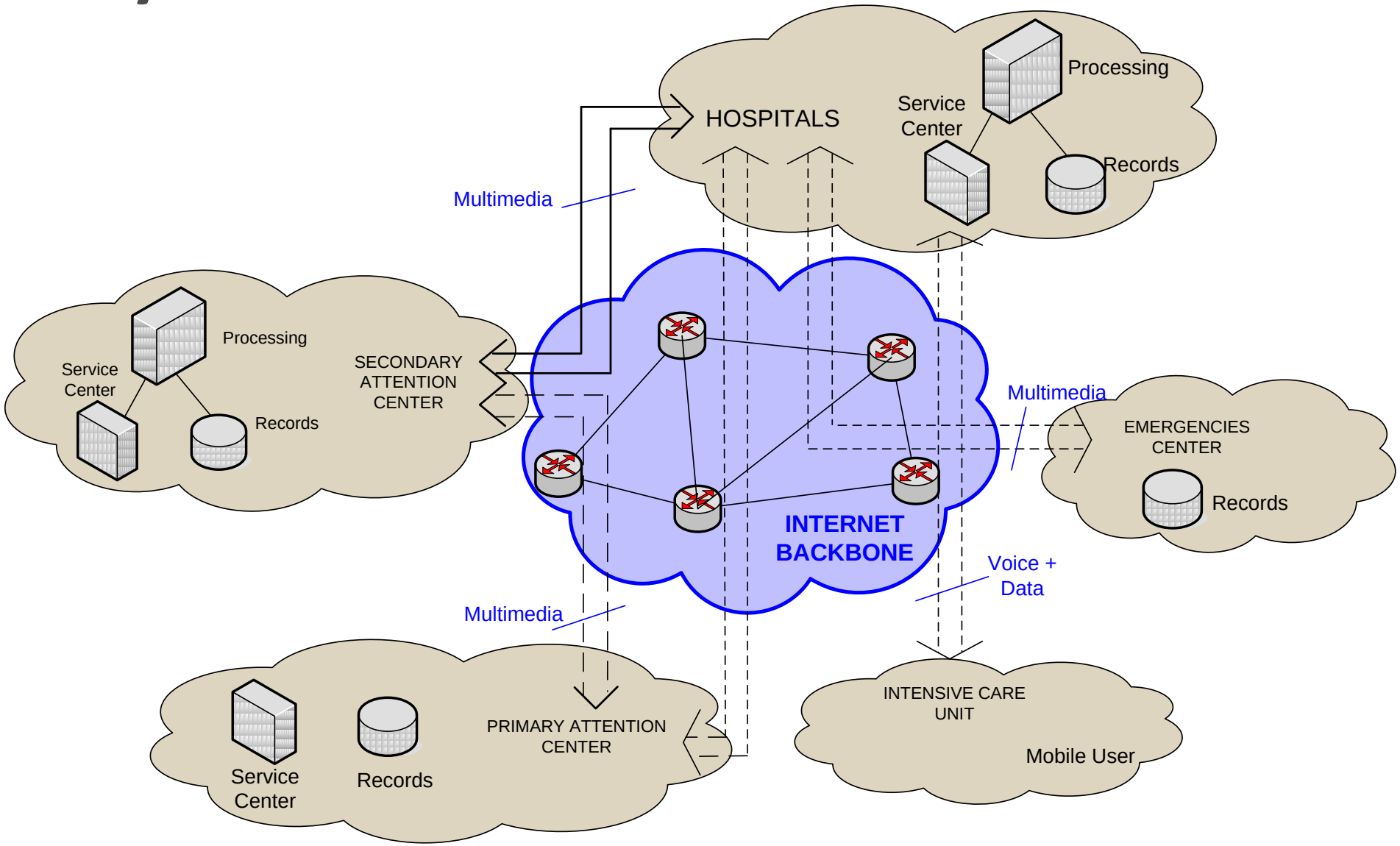
- For telemedicine
  - Audit trail of actions involving machines must be as good if not better than those involving humans
    - Non-repudiation of clinical action
    - Proper authorisation of all clinical and non-clinical actions
      - Clinical intervention
      - Clinical monitoring
- An eHealth system should be seen to perform ethically as a Turing system
  - To exhibit behaviours that make its actions indistinguishable from purely human actors

eHEALTH actors

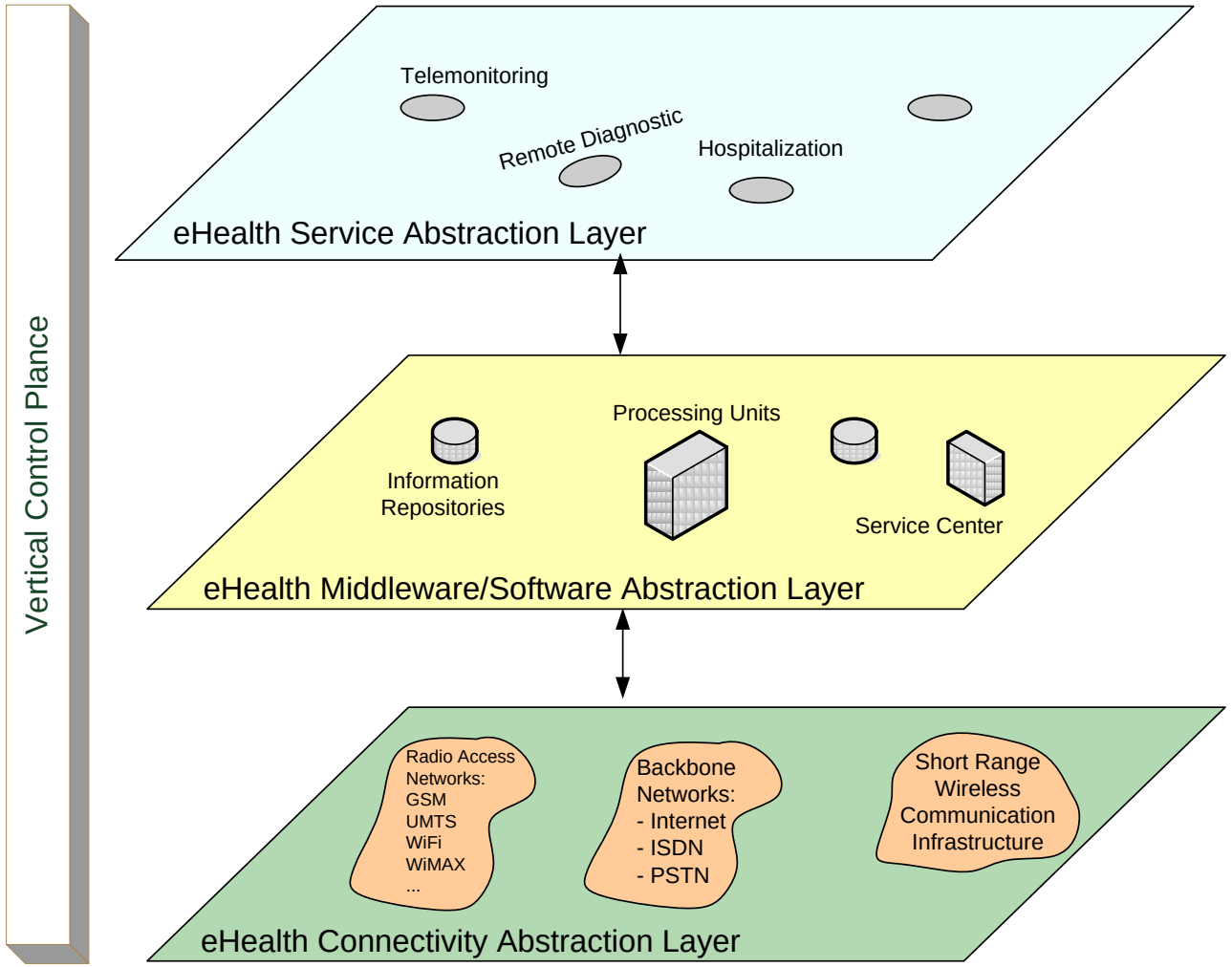


- What happens when actors are represented by a machine?
  - E.g. a doctor does not need to be a human being

eHEALTH system



eHEALTH architecture



Threats to eHealth?

- Unauthorised access to data
  - Requires identification, authorisation, non-repudiation, confidentiality (when stored and when in transit)
- Inappropriate access to data
  - Requires context processing – sometimes data has to be released but only when it is “right”
- Incorrect clinical intervention
  - By hijack of telemedicine actors (the insulin pump attack)

Black Hat hacker details lethal wireless attack on insulin pumps

By Sebastian Anthony on August 5, 2011 at 7:00 am | 31 Comments

If you thought that unlocking cars via SMS was the definition of nefarious, think again: at the Black Hat security conference, security researcher Jerome Radcliffe has detailed how our use of SCADA insulin pumps, pacemakers, and implanted defibrillators could lead to untraceable, lethal attacks from half a mile away.

Radcliffe, who is a diabetic with a wireless, always-attached insulin pump, was slightly worried that someone might hack his pump, meddle with its settings, and kill him — and so, in true hacker fashion, he has spent the last two years trying to hack it himself. Unfortunately, he was very successful. He managed to intercept the wireless control signals, reverse them, inject some fake data, and then send it back to the pump. He could increase the amount of insulin injected by the pump, or reduce it. In both cases the pump showed no signs of being tampered with, and it did not generate a warning that he was probably about to die. "I can get full remote control," Radcliffe said. "If I were an evil

So let's summarise

- Standards are essential to ensure the market for eHealth is viable
- Standards have to be realistic and address privacy, security, safety and ultimately support an ethical framework that supports patient and practitioner dignity
- ETSI has begun work on transforming experience from UNCAP into formalised standards
  - Addressing use cases
  - Addressing security, privacy and the encoding of ethics into testable logic

eHealth use cases

- The simple ones
  - The known knowns
- The complex ones
  - The known unknowns
- The really important ones
  - The unknown unknowns

Co-funded by
the Horizon 2020 Framework Programme
of the European Union

The known knowns *(things we know we know)*

- eHealth records
  - Need to be exchanged with full semantic and syntactic interoperability
  - Need to be exchanged with guarantees against manipulation and eavesdropping by unauthorised parties
    - Fairly conventional cryptographic tools available for the secure transfer
    - Identification of an authorised party not quite as clear as not all parties are authorised and some are not always authorised (context dependency)
- eHealth sensors
  - As above but with additional requirements on safety, accuracy and repeatability

Known knowns – the relationships

- Can be considered as tuples:
  - {doctor, patient}
  - {carer, cared}
  - {hospital, health-board}
  - …
- Gets increasingly difficult for real cases with more than 2 parties:
  - *Doctor* refers *patient* to *specialist* who books surgery at *hospital* with ...
  - The length of the relationship train is unkown in advance and potentially unbounded over time but at any point in time can be explicitly defined
  - Security problem is that every link in the chain has some potential for attack by manipulation of some sort – end-to-end integrity (crypto-sense) is not assured

The known unknowns *(we know there are some things we do not know)*

- Relationships
  - We know that a person will at some point in time become a patient, we don't know when or what for
  - We know that trauma will require treatment – we do not know the extent of that treatment before examination of the trauma
  - We know that at some point a patient will be prescribed a treatment of drugs but we don't know when or which drugs (in general)

  - We can identify some basic requirements to enable and protect these relationships even if we don't know the exact details in advance

Co-funded by the Horizon 2020 Framework Programme of the European Union

Known unknowns – the mechanisation of healthcare

- We know that healthcare is becoming increasingly mechanised
- We don’t know an awful lot about what is to be mechanised, when, for what classes of patient, and if it is classified as medical
- Liability and ethics
  - Where do machines fit in the ethics chain and how are they made liable for their actions?

Co-funded by the Horizon 2020 Framework Programme of the European Union

Unknown unknowns

- Cannot (obviously) be quantified

Co-funded by
the Horizon 2020 Framework Programme
of the European Union

Security issues we need to address

- Recognising longevity of the eHealth domain
  - Long term management of cryptographically protected records
    - Algorithms and keys have a short lifetime (10, 15, 20 years?)
  - Uncertainty of the parties and relationships
    - A paediatrician in early years, GPs, specialists (midwives, oncologists, …), maybe a geriatrician in the latter years – but who and where and when cannot be predefined

Where we are good and not yet good enough

- We are good at:
  - Securing 1:1 relationships (only one instance of Alice and Bob, relatively simple to identify Eve)
    - Conventional domain of symmetric cryptography
  - Securing 1:m and m:1 relationships
    - Conventional domain of asymmetric cryptography
- We are less good at:
  - Building global infrastructures for secure interoperability and interworking
- We still need to work at:
  - Securing n:m relationships, and n:m:p relationships – the core relationships of long term eHealth security

Thoughts on strategy for EP eHEALTH going forwards

- We need to prepare technical standards
  - First we need an architecture that identifies the points of control that determines where interoperability is assured
  - We need to embrace the concept of virtualisation – the future of eHealth is not in fixing a device to a location but to anywhere, anytime, any-device access
- ETSI should be ready to give authoritative guidance on the use of ICT in Healthcare
  - What are the minimum standards for interoperability? Semantic and syntactic
  - When does a device move from a wellness device to a health device?

Uncertainty for eHealth standards

- Participation
  - The eHealth market is dominated by very large procurement organisations (e.g. the UK's NICE) not currently active in standards development
  - Not at all clear if medical professionals are required participants
  - Standards encourage competitors to work together but it is not clear who the market is led by and why competitive cooperation is not an acceptable working practice for them
- Acceptance
  - A consequence of low participation is the potential of low acceptance of the standards that are published to be the establishing framework for the long term development of the eHealth market based on standards

The difficult question to go away with

- Does the world want an open, standards based, global eHealth solution?
  - If YES then support work on defining the architecture for semantic and syntactic, as well as mechanical and electrical, interoperability
  - If NO – not an acceptable answer

Thank you for listening – now for Q&A

Scott CADZOW, C3L