New Requirements for communications in eHealth

Health in IoT (HIT): Evolution of communication requirements

Applying e/mHealth and IoT:

- Monitoring
- closed loop treatment
- accessible patient data

and the evolution of communication requirements.

e/mHealth is part of IoT, health will use e/mHealth in combination with other IoT.

Cees J.M. Lanting, CSEM (CH)

Overview

Evolution of the communications requirements in Health and IoT

- **Monitoring**
- **Closed loop treatment**
- **Access to the user's medical data**
  - Normal medical data access
  - EHR
  - Emergency access
  - Large data sets
  - Big Data
- **Summary of conclusions**

Monitoring: From poor data to 'data overload'

Future eHealth monitoring in a Health and IoT (HIT) environment:

- In-body (implants, semi-implants)
- On-body (e.g. on chest, on wrists)
- Near-body (e.g. on training machine, steering wheel, seat)
- Integrated in private space (e.g. office cubicle, apartment)

Not included here:

- Equipment integrated in shared and (more) public spaces
- Clinical only health, e.g. ER monitoring etc.

Today's monitoring approach (1/2)

Poor in data

- Parameters and frequency
- Few parameters, infrequently measured
- Timing / duty cycle
  - Measurements mostly in clinic and daytime, at most in early evening
  - Measurements are snapshots
  - Infrequent measurement and assessment

Today's monitoring approach (2/2)

Quality of current monitoring:

- Measurements ad-hoc, possibly influenced by conditions, artefacts may appear; for example
  - doctors measure higher blood pressure then nurses
  - automated blood pressure measurement non-nonintrusive, artefacts likely
  - hart rate measurement not that precise

Today's monitoring approach (2/2)

Quality of wearables:

- Fashionable wearables and tools
  - Mostly low to medium quality, below state of the art
  - Comparable to 'pasta and potato cooking app': pasta and potatoes more important than health?
  - Precision and calibration lacking
    - Interest is mainly in relative, evolution measurements
    -
- The 'Openness' of smart phones, e.g. APPs, is an issue for the reliability of these devices, making them less suited for e.g. alarms

Near future monitoring approach (1/3)

Rich in data quality

- Parameters and frequency
  - Many parameters, frequent or continuous measurement

- Quality
  - Quality of measurements need to be high and constant
  - Artefacts to be detected and analysed (can be relevant or irrelevant)

Near future monitoring approach (2/3)

Rich in data volume

- Timing / duty cycle
  - Measurements are frequent or continuous
    - Cloud storage
  - Frequent or continuous interpretation / assessment possible or even necessary
    - Local pre-analysis / assessment
    - Cloud analysis / assessment

Near future monitoring approach (3/3)

Alarms

- Inclusion of generating alarms would be important benefit, but needs to be reliable:
    - Low incidence of undetected alarm cases
    - Low incidence of falls alarms
    - Requires high quality sensors and interpretation

Closed loop treatment

- Example: automatic insulin administration

- Requires high quality sensors and interpretation / assessment
- May have to be combined with alarms
- Accessible and verified parameters
  - Safe operating limits, parameters ranges
  - Operating parameters
- Logging of operating conditions

Communications requirements

Requirements depending on the device location

	Radio interface	Reliability / Resilience	Privacy / Security	Coexistence / interoperability
In-body	Medical band preferred	High	High	Coexistence w/ security systems
On-body	Open, but standards preferred	Application dependent	Medium to high	Wide range coexistence
Near-body	Open, but standards preferred	Application dependent	High if multiple users	Environment dependent
Private space	Open, but standards preferred	Application dependent	Environment dependent	Environment dependent

Requirements depending on the application

	Communication mode	Data storage	Reliability / Resilience	Privacy / Security
Monitoring	**Time to time connected**	**Large, Local and Cloud**	**Low to medium**	**Medium**
Alarms	**Always (best) connected**	**Small, Local and Cloud**	**High**	**High**
Closed loop control	**Time to time connected**	**Medium, Local and Cloud**	**High**	**High**

Access to the user's medical data (1/2)

Normal medical and para-medical data access

- Required is access and data ownership management
  - Access control and Privacy
  - Security
- A (rough) classification of data
  - Recent (semi-)fixed information (e.g. date of birth, sex, length)
  - Semi-dynamic information (e.g. weight, medication, long term average values of key parameters)
  - Dynamic information

Access to the user's medical data (2/2)

EHR and Emergency access

EHR

- Should give access to the most relevant subset of the normal medical data
  - Recent (semi-)fixed information
  - Semi-dynamic information
  - Dynamic information

Emergency access

- Should give access to a subset of the EHR
- For privacy reasons, access data should be protected by a 'break glass' protection and logging

Large data sets

- E/mHealth and HIT will generate large amounts of data
- Large data sets are typically used with regression and data mining techniques
- These datasets could be used as follows:
  - Analyse and assess the data, and draw conclusions; artificial intelligence techniques may have to be used
  - Keep parts of the data set corresponding to artefacts or incidents, and a few corresponding to average cases
  - Store data sets ‘off-line’ for use with Big Data techniques (e.g. to analyse how a patient could have contracted a certain illness)
  - Anonymise data sets and store them ‘off-line’ for use with Big Data techniques

Big Data

- Big Data will require access to large amounts of data from different sources (and possibly of different nature)
- Big Data techniques differ from ‘simple’ data mining
- In (e/m)Health datasets will likely require to be anonymised to allow to be used with Big Data techniques
- Big Data may provide valuable assistance for:
  - Identifying a set of possible diagnoses, to be confirmed with other diagnostic means
  - Identifying possible sources of infectious diseases

Communications requirements

Requirements depending on the application / data usage

	Communication mode	Data storage	Reliability / Resilience	Privacy / Security
Normal data access	On demand connected	Large, Cloud	Low	High
EHR	On demand connected	Small, Local and/or Cloud	Medium	High
Emergency	On demand connected	Cloud	High	High*
Large data sets	On demand connected	Large, Cloud	High	High
Big Data	On demand connected	Large, Cloud	Low	High (medium anonymous)

High* **High but with 'break glass' and logging functions**

Summary of conclusions

- With some exceptions, e/mHealth does not require high reliability communications and networks
  - The exceptions are:
    - Support for Alarms
    - Support for access to patient data in case of Emergencies
- e/mHealth is demanding in terms of support for data access and ownership management, hence security and privacy
- The e/mHealth requirements are remarkably, but not unsurprisingly, similar to the requirements from e.g. industry for Industry/ie4.0 and/or IoT

Thank you for your attention!