Creating Requirements and Standards for Health Data Organization and Management

Michael W. Condry, PhD

IEEE Life Fellow

IEEE Technology and Engineering Management Society,

Past-President 2020-2021

Senior AdCom, IEEE Industry Electronics Society

Member: Computer Society, Consumer Electronics, and Engineering in Medicine and Biology Society

Outline

- Situation: Advances in Technology and Medicine
- Value of accessible health data
- Producers of health data: medical and consumer
- Users of health data: individual, public health, research, business
- Typical Consumer Health System Architecture
- Proposed Data Organization
- Security considerations
- Opportunities
- Requirements
- Summary

Opportunity

Technology and Medicine

- **Medicine had made overwhelming advancements** in symptom detection and treatment methods over the past several decades.
  - Early detection of symptoms almost always gives the **most effective, least cost, and least patient impact**.

- **Advances in technologies** with AI, sensors, networking, and other digital technologies combined with medical progress has opened the door for non-invasive symptom detection with everyday life activities. These devices are exploding in the consumer market under "**Digital Health**"
  - Many these core technologies used in Digital Health devices is based on IEEE technologies including Cyber-Physical Systems and Informatics.
  - Applying Industry 4.0 technologies to human health rather than the machine/factory health
  - Opens opportunity for symptom early detection with electronic devices

- **Secured Information Organization** is critical so that the Experts can utilize this data in the most effective manner. Applies to both patient treatments and medical/business research.

- **Device Criteria, data management, suitable medical tools, security and privacy requirements and standards can lead us to a significant collection of opportunities for modern medicine.**

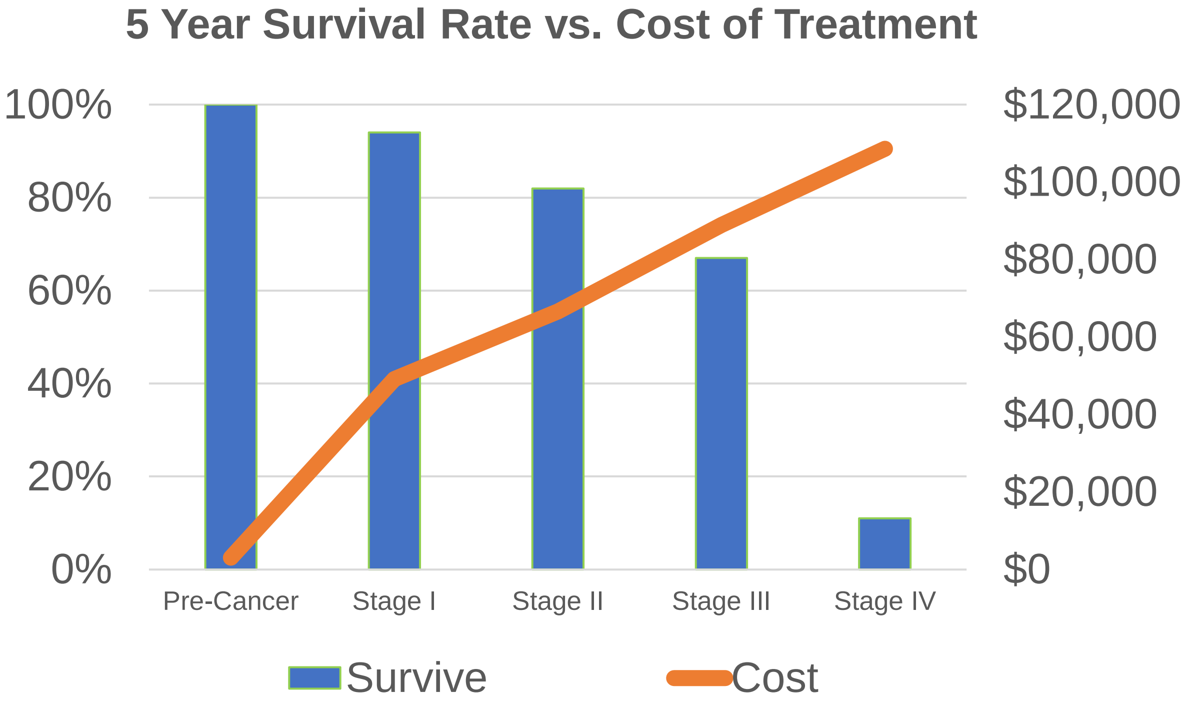
Health Data Provides Opportunities

- **Critical to the least cost and most effective treatment** relies on *early detection* and treatment of medical conditions
  - The **regularity of patient evaluation** by doctors and especially specialists **is limited** often after symptoms where the condition has advanced beyond early detection.
  - **Digital Health Consumer Devices are rapidly entering** the market testing a growing number of measurements and symptom evaluations. This opens opportunity for early detection.
- With effective, **secure** way of managing this data **doctors can receive early notification** of conditions earlier than the patent can often detect it.
  - It must be trustable by individuals, doctors, and regulators
- Organized data, with suitable privacy, can be **aggregated to study the effects of pharmaceuticals, trends, device quality, and even pandemics.**
- A data organization framework where suitable standards, criteria, and privacy can be managed to be utilized suitably is this presentation's focus.

See: M. W. Condry, "Using Requirements for Health Data Organization and Management," in IEEE Engineering Management Review, doi: 10.1109/EMR.2021.3100418.

Early Discovery nearly always gives the best solution

Example Colorectal Cancer, consider cost, effectiveness vs. discovery time



Source: Kakushadze, Zura, Rakesh Raghubanshi, and Willie Yu. "Estimating Cost Savings from Early Cancer Diagnosis." Data 2.3 (2017): 30. Crossref. Web.

Making the Value

- **Critical to the least cost and most effective treatment** relies on early detection and treatment of medical conditions
- The **regularity of patient evaluation** by doctors and especially specialists **is limited** often after symptoms where the condition has advanced beyond early detection.
- **Digital Health Consumer Devices are rapidly entering** the market testing a growing number of measurements and symptom evaluations.
- With effective, secure way of managing this **data doctors can receive early notification** of conditions earlier than the patent can often detect it.
- In addition, organized data, with suitable privacy, can be **aggregated to study the effects of pharmaceuticals, trends, and even pandemics.**
- To utilize we need a framework where suitable standards, criteria, and privacy can be managed to be utilized by individual doctors as well as researchers in the aggregate.

Producers of Health Data

- **Traditional Medical Records**
  - Organized digital systems, such as Epic
  - Simple written records
- **Consumer Health Devices** – both typical measures and medical symptom testing
  - Wearables (Apple, Fitbit, etc.) typically measure basic readings
    - Temperature
    - Heart Rate
    - Blood Oxygen
    - EKG
  - Home devices can measure readings and symptoms
    - Blood Glucose (Dexrom)
    - Blood Pressure (ONRIB)
    - Toilet Monitor to detect gastrointestinal symptoms, e.g., Colorectal Cancer (ClinicAI)
  - More every day!!! **Providing electronic tests potentially equal to the laboratory or doctor testing**

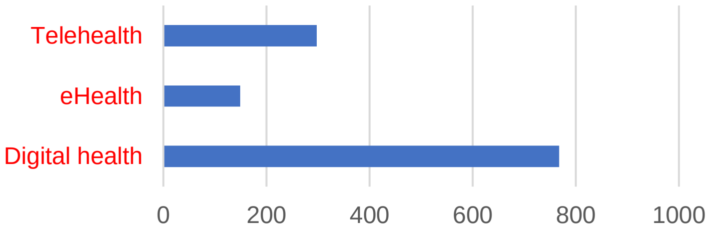
Consumers of Health Data

- **Individuals**
  - Organized digital systems, such as Epic
  - Simple written records
- **Doctors**
  - For the patient
- **Medical and Pharmaceutical Research**
  - Academic studies
  - Business Product evaluation
- **Industry**
  - Employee health and exposures
- **Public Health**
  - An <u>international</u> challenge
- **Consumer Health Devices**
  - Product quality evaluation

Consumer Health Devices – A few examples and notes

- **Wearable devices** that can detect selected symptoms and measures
  - Dexcom Glucose Monitor
  - ONRIB blood pressure monitor
  - Apple watch with EKG, new Apple 7 Watch
- **Home devices** detecting symptoms in the home
  - ClinicAI toilet monitor for GI symptoms
  - Omron connected blood pressure monitor

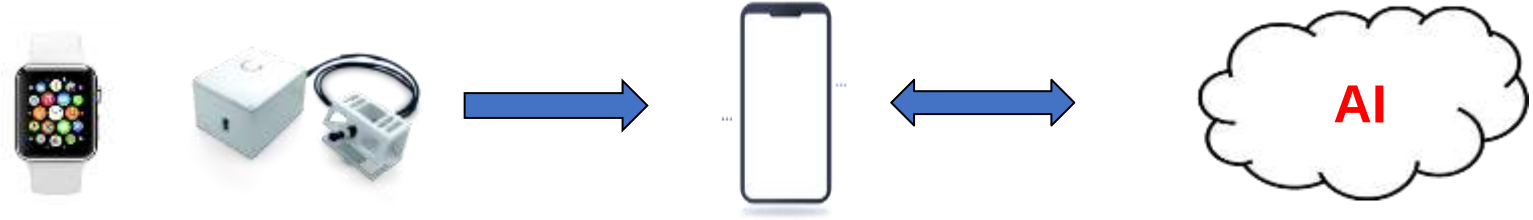
Startups in the digital health arena



- Some devices provide measurements common to medical use (e.g., glucose level and temperature) others provide symptom indicators (e.g., Colon cancer indicators).
- Many more are coming **detecting blood chemistry matters, waste analysis, etc.** – performing tests and measurements typically done in the medical laboratory.
- Many use technologies such as **AI and sensors following Cyber-Physical designs to determine symptoms**
- Yes, there is clearly an issues of data criteria quality as well as organization

M. W. Condry and X. I. Quan, "Digital Health Innovation, Informatics Opportunity, and Challenges," in IEEE Engineering Management Review, vol. 49, no. 2, pp. 81-88.

Typical Consumer Digital Health Architecture



Sensor/ Data System

- Multiple Sensors
  - Optical, Radio, etc.
- Simple Processor
- Local Communication
- User Identification
  - Bluetooth

Edge Device

- Package data
- Encryption
- Internet to Cloud
- Message to User
- Data for sharing

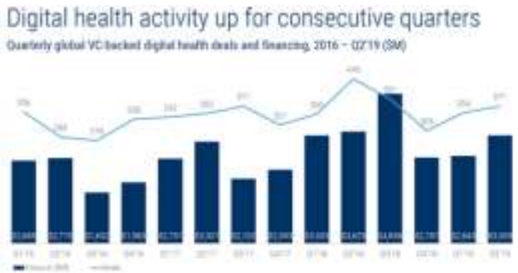
Cloud

- AI engine
- Search for Multiple Symptoms
- Communicate with User
- Optional Medical Communication
- Continuous Improvements
- Record Keeping

Commonly a Cyber-Physical System Architecture

Observations

- Devices provide **both symptom detection for a multiple conditions and health measures** operating in a normal non-invasive daily environment.
  - Internal data can be proprietary, but External data must be standard for the test
- Information **needs to be clear for medical usage**, with no single vendor dependence.
- Devices need **measure of quality criteria** that scales accuracy.
- Devices may use proprietary technologies in order to detect their measure or symptom, however the **data to be used must be both secured but available** to any appropriate system with the user's consent.
- There are business challenges to assure vendor cooperation in the overall complex picture.



Digital Health Activity continues to grow and expand market opportunities

M. W. Condry and X. I. Quan, "Digital Health Innovation, Informatics Opportunity, and Challenges," in IEEE Engineering Management Review, vol. 49, no. 2, pp. 81-88.

Digital Health Data Informatics

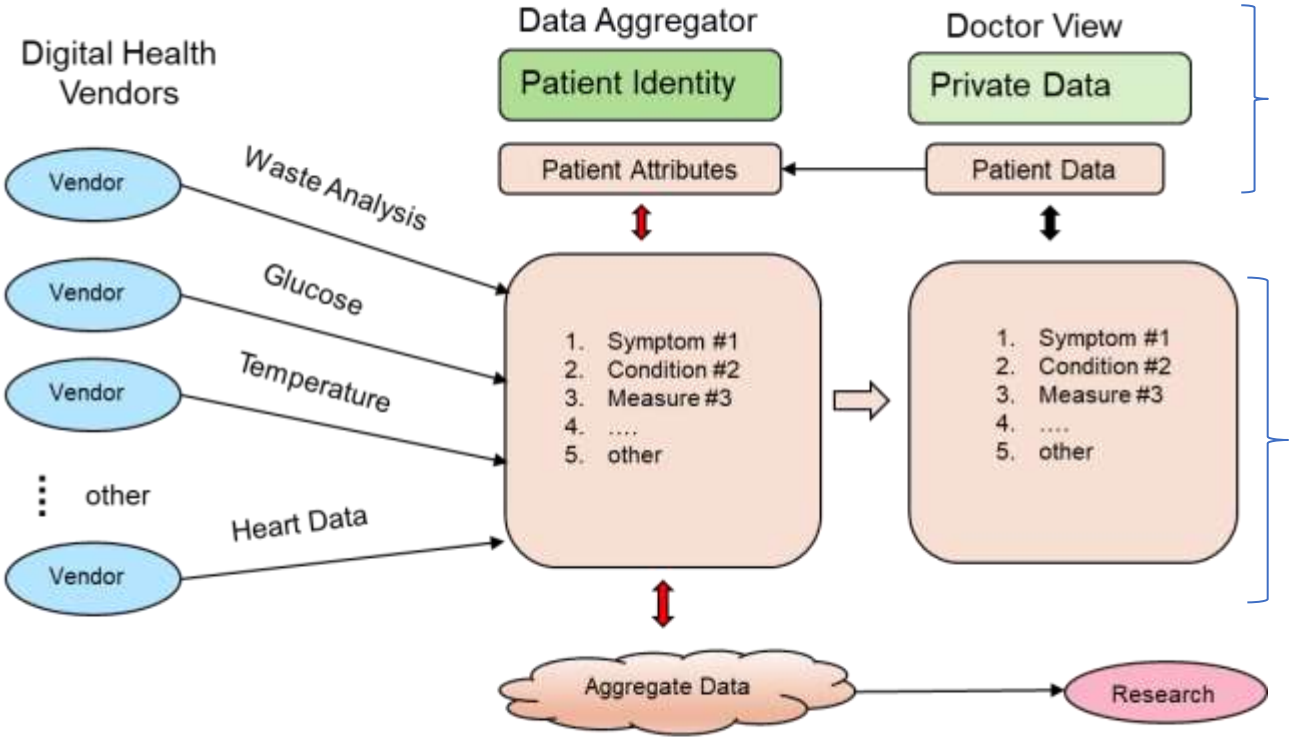
How the data is managed, moved, maintained, accessed and secured

- The proposed framework structures how the digital health data can be managed, moved, maintained, accessed and updated.
- Our framework groups them into 3 service categories:
  - **Consumer Digital Health devices** provides health measures and symptom detection devices
  - **Data Aggregator Service a service**
    - Exchange service between consumer devices and medical groups
    - Source for medical data access from all sources
    - Regulated to maintain security and privacy
  - **Medical Group information** service that is used by the patient’s medical professionals for the patient’s doctor’s usage, tracking, updating, etc. This exchanges data with the Data Aggregator.
- Situations such as moving between Medical Groups and even Data Aggregators must be managed, and services must be approved by the consumer/patient and medical group.

Note this is service structure, products may combine at the vendor level

Data Organization Model

Patient



Digital Health Vendors

Vendor

Vendor

Vendor

⋮ other

Vendor

Waste Analysis

Glucose

Temperature

Heart Data

Data Aggregator

Patient Identity

Patient Attributes

1. Symptom #1
2. Condition #2
3. Measure #3
4. ….
5. other

Doctor View

Private Data

Patient Data

1. Symptom #1
2. Condition #2
3. Measure #3
4. ….
5. other

Aggregate Data

Research

Private

Can be Shared

Sharing depends on Authentication

Data Management Observations

- **Consumer devices can come from multiple vendors**, information data standardized by measure
- The doctor sees this information along with patient's medical records and identification. They are expected update patient's attribute data. **System must be reasonable for the doctor in terms of effort and provide valued return.**
- Note each "player" will share some data with the aggregator and retain some for additional research requests – this is critical for business opportunities
- The Data Aggregator service organizes operates under both consent of the consumer/patient and medical expert, that includes individual attributes such as medical conditions and medications;
  - **Security and Privacy are the key responsibility of the Data Aggregator**
  - **Authentication** establishes what data can be seen by whom and managed by the Aggregator
- Consumers need ability move between medical groups and data aggregator services without loss. Likely, the medical group will likely select preferred aggregator.
- Tools must exist to simplify any interface between the medical community and the aggregators.

Data Aggregator Key Roles

- Data Aggregators **organize the data from multiple sources**. Patient identity must be kept private to the patient and doctor. Aggregator can request additional data for research from contributors.
- **All information is shared to the patient's doctor** to align with patient's medical records and identification. They may update patient's attribute data the aggregator. Must be reasonable for the doctor in terms of effort and provide valued return.
- Association between data and patient can only exposed to the patient and doctor.
- **Aggregate Data about the patient may include**
    - Physical data (age, gender, etc.)
    - Region data (location)
    - Medications
    - Observed conditions
- **Standards, Security and Privacy requirements are needed** for suitably collect data and share aggregate information.

Security Model and Requirements

- **Private Identity information is retained in a separate are than the generic** aggregate data about the individual. Likely a vendor-based code is used to link the two data records.
- **Identity is only known to the aggregator, doctor, and individual**. No access to the private data except doctor and patient.
- **Blockchain** is central to aggregate data security.
  - Note again, private data and aggregate are maintained separately.
- **Access depends on authentication**
  - Device vendors provide data to aggregator
  - Doctor provides data to aggregator, marking private from aggregate
  - Additional access depends on usage
    - Medical and Pharmaceutical research
    - Research on effectiveness of consumer device measures
    - Public Health
    - International Sharing

Business Roles: Data is most Valuable

- The **digital health devices retain longer term records** for the individual, likely giving regular summaries (such as mean, minimum and maximum measures over a period like 14 days) to the data aggregators.
- The **data aggregator keeps the aggregate information** from the devices and medical professionals. Record keeping is time limited.
  - Requests for longer data return to device vendor or medical professionals that retain additional data.
  - Revenue for requests is shared across the providers
  - Aggregate data requests for research and studies come to the data aggregators
  - Data security and privacy are critical roles, Blockchain offers a technology to control both
- The associated **medical group retains records and provides some data** to aggregator vendors.
  - The medical professional knows the exact conditions of each patient and their associated "codes"
  - A group may choose to work with a limited number of vendors.
  - Tools must greatly limit any burden on medical professionals to engage, and the return must be better patient care

Brief Opportunities

- **Individual care** – remote analysis and early detection notifications. Telemedicine.
- **Medical and Pharmaceutical Research** –treatment tracking, broader symptom and cause studies, side effects of medications
- **Consumer device evaluation** – steps toward a measurable system of quality
- **Public Health**
- **International options** – tracking pandemics
  - Being able to sample populations where testing was done and select data from tested individuals.
  - Using AI and other techniques determine criteria associated with positive cases. Likely some indicators may come from consumer devices as well as generic indicators (age, weight, hypertension, …).
  - Notify the medical community of indicators in the positive groups to narrow down the ones needing testing and isolations.
- **Tools** to address situations
  - Tools for international sharing of medical situations
  - Doctor’s tools for medical records to aggregator

Requirements Summary

- **Digital Health Devices**
  - Internal data and communication can be proprietary
  - External data (or aggregator) must be standard across all vendors
- **Data Informatics requirements are needed** for maximum and safe usage
  - Organized to protect identity but allow for most research with clean data
  - Individuals can move across aggregators, no one vendor solution
  - Clean separation Private and Aggregate data
- **Medical Records** need to be shared and updated regularly
  - Tools must simply the process of limited sharing of medical records for all doctors and medical groups
- **All parties**, including medical research, engineering, industry, and regulators **need to develop these requirements** together.
- **Security with Trust is critical for success**
  - Aggregate service is key to privacy management (and selling the data)
  - All users including Doctors and Individuals must <u>trust</u> the system

Summary

- **Digital Health Devices -** rapidly growing market with potentially valuable data
- **Data Organization** for maximum and safe usage
- **All parties**, including medical research, engineering, industry, and regulators **need to develop these requirements** together.
- **Security with Trust is critical for success**
  - Dividing Private and Aggregate data
  - Aggregate service is key to privacy management (and selling the data)
- **Significant Business opportunities as well as better humanity health**
  - Individual Health with early detection
  - Research starting with Aggregate services including testing consumer device quality
  - Domestic and International Public Health for pandemics and other studies
- All users including Doctors and Individuals must trust the system

For more see: M. W. Condry, "Using Requirements for Health Data Organization and Management," in IEEE Engineering Management Review, doi: 10.1109/EMR.2021.3100418.