Systems integrating self-collected health data by patients into EHRs and medical systems: a State-of-the-art review

Giordanengo Alain[2,3], Bradway Meghan[1,3], Muzny Miroslav[3,4], Ashenafi Zebene Woldaregay[4], Hartvigsen Gunnar[2,3], Årsand Eirik[1,3]

[1] Department of Clinical Medicine, UiT The Arctic University of Norway, Norway

[2] Department of Computer Science, UiT The Arctic University of Norway, Norway

[3] Norwegian Centre for E-health Research, University Hospital of North Norway (UNN), Tromsø, Norway

[4] Spin-off Company, Research Results Commercialization Center, The First Faculty of Medicine, Charles University in Prague, Czech Republic

Abstract

This template may be used for articles in journals or conference articles. Differences may occur, of course, and this template is only a guide how it may appear. Patients are being more and more autonomous in their disease management by collecting, viewing and analyzing health data themselves with the support of sensors, wearables and smartphone apps. Self-collected health data can be used by the medical environment to provide more tailored and efficient therapies. This paper presents a state-of-the-art review (per April 2017) on systems integrating self-collected health data by patients into Electronic Health Record (EHR) systems and other medical systems assessable for the clinicians at the point of care.

Keywords

Self-collected data, Wearable, Sensor, EHR, Integration

1 INTRODUCTION

Patients are increasingly using m-health services and applications for storing, viewing and analyzing their self-collected data, as an answer to geographical, temporal and organizational barriers in healthcare (Tachakra et al., 2003). Studies have showed that self-collected data and self-management is beneficial and effective for managing chronic diseases, especially in diabetes (Norris et al., 2001). Moreover, wearable devices and sensors become more and more important for long-term self-management (Haghi et al., 2017) by allowing automatic data collection without the intervention of patients. Also, systems permitting cooperation between empowered patients, collecting their own health data, and medical workers, have been proved to have a positive effect on their satisfaction managing patients' chronic diseases (Peleg et al., 2017) by providing patients mentoring and knowledge they will not be able to gain on their own. However, these studies are limited to specific cases and relies on custom cloud systems and on specific sensors to deliver their services. Therefore, these studies do not present a standard integration between patients' and EHR systems, i.e. enabling only exchange of some kind of data in separate systems. This is curbing cooperation between patients and medical workers, leading to security, transparency and privacy issues. Also, needing to relate to vendor-specific systems implies that patients cannot choose freely among systems or sensors that suit them the most, according to their experiences or preferences.

This paper presents a comprehensive review of the state of the art of systems that directly integrate patients' self-collected data into EHRs and similar medical systems, and the implications on security and privacy of such systems.

The results will be used as a basic set for the design and the development of a system allowing self-collected health data transmission between diabetes patients and healthcare institutions systems in Norway.

2 METHODS

2.1 Scientific literature search

The scientific literature search followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology. Keywords and the search query were selected through brainstorming sessions with the authors. Terms including "Fast Healthcare Interoperability Resources (FHIR)" or "OpenEHR" were omitted because they represent solutions for solving interoperability issues and usually do not include specific systems as was the target of this review. Considering the novelty of sharing patient-collected data, only peer reviewed articles published after 2012 were considered. The following online databases were searched: Pubmed, ACM Digital Library, IEEE Xplore and Scopus. The search query has been adapted for each online database considering their operational functions and restrictions and was run using the metadata fields: title, abstract and keywords.

All scientific papers resulting from the database searches were imported into Rayyan (Ouzzani et al., 2016), a web

Paper from the 15th Scandinavian Conference on Health Informatics SHI2017, Kristiansand, Norway, 29 - 30 August.
Conference Proceedings published by Linköping University Electronic Press.

service allowing a structured review of titles and abstracts, which was used by the authors for improving collaboration and quality assurance of the process.

(EHR or "Electronic Health Record" or "Health System" or "Medical System" or "Health Information System" or CDS or "Clinical System" or "Clinical Decision Support" or "Clinical Decision Support System" or EMR or "Medical Records" or EJS or "Electronic Journal System")
and
(interoperability or communication or exchange or integration or collect or transfer* or shar* or stor* or gather* or record*)*
and
(wearable or mhealth or phone or apps or "Mobile health" or sensor)

Figure 1: Search query and keywords used for the scientific literature review

Two of the coauthors identified irrelevant articles using metadata fields while considering inclusion and exclusion criteria. The first author then reviewed the remaining articles for inclusion based on relevance of the full texts.

Inclusion and exclusion criteria

To be included in the review, the paper should describe a solution that facilitate a direct integration of patients' self-collected data into the healthcare system, pre- or at the point-of-care, or in real-time.

Studies are included only if they describe an evaluation, an implementation, a review, a working solution or prototype transferring patient self-collected data into medical systems, or are related to the security or privacy for accessing and managing the medical data self-collected by the patient by such system.

Studies that required healthcare workers to log onto a service outside their healthcare institution's EHR system in order to consult the data (e.g. a cloud-based data consultation service such as a Personal Health Record System (PHR) on Internet) were excluded. Several reasons justify this exclusion:

1. Healthcare workers are not willing to spend time to use separate Internet tools (Bradway et al., 2017).
2. The healthcare workers do not have knowledge of all relevant cloud-based or Internet-based solutions available, and how to use them(Bradway et al., 2017), and.
3. The data from such systems is usually not directly transmitted to the healthcare system (often the healthcare workers must take screenshots or copy the data into their EHR system manually).

However, studies including PHRs directly integrated within EHRs, were included, being part of the healthcare institution system.

In addition, the papers must describe data that is collected by the patient themselves using their own system, e.g. apps or sensor systems, which could be obtained from a healthcare or a research institute. Studies relying on "collector agents", typically medical workers visiting patients at home for collecting data, were also excluded.

Data categorization and data collection

The information mined from the papers was organized into categories, defined by the authors through brainstorming sessions, and were used to present an aggregated overview of the current situation:

1. *Patient data sources*: systems, e.g. sensors, apps or aggregators, that allow patients to collect data themselves.
2. *Data collection*: whether data sharing required automatic or manual interaction from the patients or the medical workers.
3. *Patient data type*: whether the data collected from the patient is structured (e.g. measurements values with units) or un-structured (e.g. videos or general notes).
4. *Interoperability*: which standards the system is using for data transfer, representing clinical documents, and/or terminologies (e.g. SNOMED-CT). Note, again, that for this review, we focused only on interoperability between the patient system and the medical system.
5. *Security*: which security protocols or approaches have been followed for either collecting, sharing, storing or analyzing the data; for authenticating patients; or for ensuring privacy.
6. *System services*: the types of services, applications or state of development of the project (e.g. proof of concept, prototype, or commercial).

The evaluation and analysis were based on these categories and each paper is expected to fulfil at least one of them to be included.

2.2 Grey literature search

The search query (**Error! Reference source not found.**) was also applied to both the Google and Bing search engines. The same inclusion and exclusion criteria were applied, but was extended to different type of results, including webpages and business documents. The data categorization, data collection and literature evaluation followed the same procedure.

3 RESULTS

3.1 Combined reviews on literature

As shown in **Error! Reference source not found.**, 811 articles were identified from the scientific literature and 4 from reviews of commercial product and business reports. Eighty-three duplicates were identified and removed in Rayyan after importing the articles. Two of the co-authors reviewed the resulting articles' titles and abstracts independently based on the inclusion and exclusion criteria. Discrepancies (i.e. when articles were included by one author but excluded by the other) were resolved through discussion. In total, 682 articles were excluded, leaving 50 articles for full-text assessment. The first author

then identified n=40 articles for exclusion based upon the following reasons:

- Out-of-scope study or review (e.g. focus only on reducing latency between mobile phone and healthcare systems) (34).
- Inaccessibility of the full-text article (3).
- Inappropriate study objectives and methods: description or testing of a model for integrating self-collected patient data that does not have either a working prototype or any low-level description of such system for replication (2).
- Inappropriate technology usage, e.g. use of Short Message Service (SMS). This technology for chronic disease management restricts the patient regarding how they enter and exchange data (1).

At the end, 10 articles were included for final data collection.

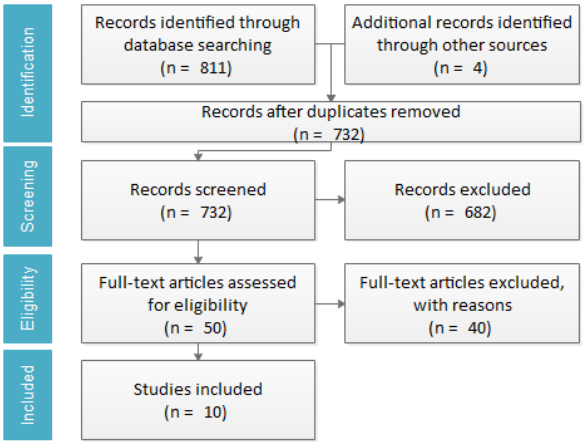

Figure 2: PRISMA flow diagram

3.2 Data Extraction from included articles

The evaluation and analysis of the included articles (Table 1) is based on the categorizations described previously in the methods section.

Functional solution

To the best of our knowledge, there were no standard and stable end-to-end systems permitting patients to share their own-collected data with EHR systems when this review was completed (April 2017). Eight of the papers presented a functional solution that described the design and usage of custom interfaces, Application programming interfaces (APIs), apps and/or restricted sensors in order to provide their services. Only three described an end-to-end system.

The closest solution to a fully operational system is the pilot described by Kumar et al. (2016), in which glucometer measurements were collected automatically by a specific IOS application, Share2, from the Dexcom G4 glucometer sensor worn by the patient. The data is then transmitted to HealthKit, then transmitted to the EPIC EHR system through MyChart app, a patient portal integrated with EPIC, to display data. This system requires explicit consent of the patient before allowing data transfer between the HealthKit and MyChart. Unfortunately, this system includes some limitations:

- Time consuming: the one time setup requires to spend between 45 to 60 minutes in addition to the clinic visit;
- Performance issue: with up to 288 glucose readings per day, MyChart standard flowsheet was unable to visualize the patient trends over weeks to months and the MyChart app displayed errors and froze due to the high volume of data communication. These errors were fixed by limiting the import of data only from the preceding 24 hours and developing a custom web-service in the EHR system.

The second end-to-end system was a proof of concept (POC), described by Marceglia et al. (2015), where data was collected from an IOS app and sent to OpenMRS EHR through the Clinical Document Architecture standard (CDA), and using data related to heart failure. The opposite flow (from EHR to mobile app) was implemented as well. Unfortunately, this POC was validated using a simulated environment only.

The third end-to-end system, presented by Pfiffner et al. (2016), focused on gathering self-collected patient data for research purposes. To do so, the system relies on Ctracker, an IOS created by this project, in combination with ResearchKit and Healthkit. On the medical side, the solution relies on the Informatics for Integrating Biology and The Bedside (i2b2), which is a research framework aiming to facilitate the design or tailoring of therapies and integrated in academic health centers. While i2b2 is not an EHR system, it is part of medical systems and therefore fulfills our inclusion criteria. Surveys and HealthKit data are collected. FHIR is used to manage the data exchange between all of these components.

Five articles dealt with systems that do not provide an end-to-end solution, but instead describe interfaces to missing components. For instance, the self-managed mobile personal health record system (SmPHR) described by Park et al. (2016) relies on the personal area network (PAN) and the wide area network (WAN) interfaces defined by the Continua standards to collect data from sensors and transmit them to health systems. Blood pressure, body weight, blood glucose and oxygen saturation are collected from sensors paired to the SmPHR and transmitted into a PHR. Other studies (Leijdekkers and Gay, 2015, Gay and Leijdekkers, 2015) describe the same smartphone application, MyFitnessCompanion, which aggregates fitness data from different online services (e.g. FitBit), Bluetooth Low Energy (BLE) and Universal Serial Bus (USB) devices and rely on other online services like HealthVault for *potentially* sharing data with EHR systems, using Health Level Seven (HL7) standard family for ensuring interoperability. The learning health system PORTAL (Young et al., 2014) relies directly on the EHR systems part of their network for gathering patient data which *could* be self-collected. The personal mobile health record system (PmHR) proposed by Song and Qiu (2016) relies on a PHR cloud solution for sharing data, using CDA documents in

combination with Snomed and Logical Observations Identifiers, Names, Codes (Loinc). Blood glucose, blood pressure, heart rate and heart rate variability, electrocardiography (ECG), weight, height and temperature are measurements used by the app.

On the 8 studies, 7 mention using apps as a source for data gathering, 6 reference using managers or aggregators, 5 declare using sensors. An EHR and a Cloud system are also mentioned 1 time each. The data collecting process is automatic in 7 cases, and none but one describes a required manual setup to access the services. The data collected is structured in 6 cases, unstructured in 1 and both in 1.

Security and privacy

Concerning the privacy, Hordern (2016) proposes an analysis of the protection of health data. According to this study, Health data is defined as personal data including *medical aspect of a person such as test results, doctors' notes, medical research* but as well as data collected by self-management sensors. However, a legal framework is lacking for Health data due to its diversity of services (e.g. smartphone apps, cloud, big data, and sensors). However, in a general approach, there are three requirements:

- Explicit consent from the patient to process health data, except if this data is necessary for carrying out obligations or in case of emergencies or medical diagnosis;
- A transparency notice informing the patient which, how and why the health data has been collected, and how it will be used;
- Full access to the health data collected, for allowing patients to consult and move data between providers.

The study also highlights the need to have controllers and processors. A controller is an entity which collects data for its own purposes (e.g. hospital) and is responsible for legacy compliance. A processor is a third party entity that uses personal information on behalf of the controller. This should comply with the controller instructions regarding health data storage and process, which requires a contract. This adds complexity: if the data is collected by a hospital directly from a patient, the hospital is a controller, in which case, it is straightforward to comply with the laws. However, in a situation where a sensor, an app, a cloud solution and an EHR are required to mutually share self-collected patient data (example described in the previous section), there are several unanswered questions: is the EHR, the app or the cloud service the controller and provider? Should all of these entities have a contract with the patient or merely between each-other? Should the end service (EHR) validate the whole exchange?

Concerning the security, Rubio et al. (2016) propose an analysis of and possible improvements for the security of the European standards regarding communications between medical, health care and wellness devices, sensors or systems (CEN ISO/IEEE 11073), especially involving personal health data (X73PHD). In our case, the highest level security described in this study corresponds to our criteria: level annotated layer 2.5 and it describes solution '*intended for applications which may require integration with EHR systems […] intended for patient remote monitoring, follow-up and laboratory-test'*. The study by Rubio et al. (2016) proposes the use of improved Integrating Healthcare Enterprise (IHE) profiles in 4 security-related categories: user identification, device identification and authentication, time coordination and encryption and proposes solutions and algorithms for doing so such as Twofish, RSA2048 or ECDSA256.

Considering that patient data could be stored on servers outside of the European Union (e.g. Healthvault or FitBit servers) and the huge amount of services/apps available, implementing a service for sharing self-collected patient data with EHR systems compliant with European privacy and security rules is extremely challenging.

Semantic interoperability

The semantic interoperability ensures that different systems are able to exchange, understand and analyze the data correctly by using standards for communication, medical representation (documents) and terminologies (Mead, 2006).

Among the previous 8 studies, 6 of them are describing the use of the HL7 family to ensure interoperability (4: CDA/ Continuity of Care Document (CCD)), 1: FHIR, 1: Continua WAN). Snomed-CT is described in 3 of them, 2 mentioned using the International Classification of Diseases (ICD), 1 Digital Imaging and Communications in Medicine (DICOM) and 1 LOINC. Surprisingly, there is no implementation of archetypes or the OpenEHR approach in these studies, even if there are mentioned (Marceglia et al., 2015).

However, using the same standard family is not enough for insuring interoperability, but the discussion is outside of the scope of this paper. None of the solutions described in the previous studies provide interoperability with each other's, and relies upon a custom approach as described in the previous section.

4 DISCUSSION

The focus on Decision Support Systems extracting data from patient self-collected health data systems and EHRs could explain the limited number of relevant papers identified in the scientific literature review (10 of 732), on top of the reasons cited in the results section.

Also, the trend of patients managing their diseases in the palm of their hands with health applications, e.g. PHRs, sensors and hacking commercial systems, which collect data without using proprietary solution, for privacy reason (Gay and Leijdekkers, 2015), is growing (Muzny, 2017). New sensors are developed and launched on the market at a more rapid pace than ever before, and more types of data can used directly by patients. One example is Tytocare (http://www.tytocare.com), which is providing new sensors for examining the ears, throat, heart, lungs, abdomen, skin, and capturing heart rate and temperature. New open source operating systems for wearables and sensors such as Google Wear will also help standardize the

ecosystem and improve the semantic interoperability between components in the future. Even if there is no standard exchange between patients' self-collected data system and EHRs today, the authors believe this situation will evolve quickly. Businesses and researchers are more frequently acknowledging the new trend where patients are the center and key decision makers of their health services. This will lead to the design of new medical protocols and procedures in which patients are more empowered (Mantwill et al., 2015, Lamprinos et al., 2016). Additionally, businesses will increasingly shape their communication around the patients themselves (e.g. "With the Patient at the heart" catchphrase of EPIC Systems, http://www.epic.com). Even legal authorities are aware of these evolutions, but have not yet been able to provide an operational legal framework for the security and privacy for protecting patients and health institutions. It is also necessary to protect such systems against data forging(Hordern, 2016), which could lead to medical errors, and hacking of wearables, and subsequent risks to patients including death in certain circumstances (Halperin et al., 2008).

5 CONCLUSION

Our findings indicate that there are no standard and stable end-to-end system permitting the sharing of patient-collected data with EHR systems when this review was completed (April 2017). We suggest that this may be due to:

- Business models that currently only describe closed, proprietary and custom applications, interfaces and protocols;
- A lack of legal framework concerning the security, privacy and transparency of systems dealing with self-collected health data. The European General Data Protection Regulation (GDPR) can provide partial answers to the questions cited in the results section, but will not be enforced before next year;
- The complexity of integrating international and external aggregators or applications in such system, and the complexity of assuring a semantic interoperability between all actors;
- The large amount of patient-collected data that re-quire more coordinated and efficient ways of analyzing and following up this new type of information.

However, the variety of data collected from sensors and wearable is expected to be important, from fitness activity to more advanced medical data such as ECG and blood values (glucose, lipids, etc.). Patients can now buy more and more sensors, which are not just limited to activities trackers and smartwatches anymore, but include a wide range of exotic solution like e-clothes (e.g. smart-bras, smart-socks, smart-caps) and medical sensors such as HRMs or CGMs. Unfortunately, most of the businesses manufacturing these sensors close their solutions using private protocols and standards forcing patients to use their in-house developed applications to consult the data. This has led to a situation where patients are not waiting for the businesses to open-up anymore, and hack the protocols to extract, share and use the data the way they find to be the best for their health challenges.

6 REFERENCES

[1] Bradway, M., Giordanengo, A., Årsand, E. & Grøttland, A. 2017, Co-design Workshop on Integrating patients' self-collected data into clinical systems: identifying opportunities and challenges for clinicians. Nasjonalt senter for e-helseforskning.

[2] Gay, V. & Leijdekkers, P. 2015, Bringing health and fitness data together for connected health care: Mobile apps as enablers of interoperability. *Journal of Medical Internet Research,* 17.

[3] Haghi, M., Thurow, K. & Stoll, R. 2017, Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices. *Healthcare Informatics Research,* 23**,** 4-15.

[4] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T. & Maisel, W. H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. 2008 IEEE Symposium on Security and Privacy (sp 2008), 18-22 May 2008 2008. 129-142.

[5] Hordern, V. 2016, Data Protection Compliance in the Age of Digital Health. *European Journal of Health Law,* 23**,** 248-264.

[6] Kumar, R. B., Goren, N. D., Stark, D. E., Wall, D. P. & Longhurst, C. A. 2016, Automated integration of continuous glucose monitor data in the electronic health record using consumer technology. *Journal of the American Medical Informatics Association : JAMIA,* 23**,** 532-7.

[7] Lamprinos, I., Demski, H., Mantwill, S., Kabak, Y., Hildebrand, C. & Ploessnig, M. 2016, Modular ICT-based patient empowerment framework for self-management of diabetes: Design perspectives and validation results. *Int J Med Inform,* 91**,** 31-43.

[8] Leijdekkers, P. & Gay, V. 2015, Improving user engagement by aggregating and analysing health and fitness data on a mobile app. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* 9102**,** 325-330.

[9] Mantwills, S., Fiordelli, M., Ludolph, R. & Schulz, P. J. 2015, EMPOWER-support of patient empowerment by an intelligent self-management pathway for patients: study protocol. *BMC Med Inform Decis Mak,* 15**,** 18.

[10] MarcegliaA, S., Fontelo, P., Rossi, E. & Ackerman, M. J. 2015, A standards-based architecture proposal for integrating patient mhealth apps to electronic health record systems. *Applied Clinical Informatics,* 6**,** 488-505.

[11] Mead, C. N. 2006, Data interchange standards in healthcare IT--computable semantic interoperability: now possible but still difficult, do we really need a better mousetrap? *J Healthc Inf Manag,* 20**,** 71-8.

[12] Muzny, M. 2017, Wearable Sensor Systems with Possibilities for Data Exchange. Nasjonalt senter for e-helseforskning.
[13] Norris, S. L., Engelgau, M. M. & Venkat Narayan, K. M. 2001, Effectiveness of Self-Management Training in Type 2 Diabetes. *A systematic review of randomized controlled trials,* 24**,** 561-587.
[14] Ouzzani, M., Hammady, H., Fedorowicz, Z. & ElmagarmidL, A. 2016, Rayyan-a web and mobile app for systematic reviews. *Syst Rev,* 5**,** 210.
[15] Park, H. S., Cho, H. & Kim, H. S. 2016, Development of a multi-agent M-health application based on various protocols for chronic disease self-management. *Journal of Medical Systems,* 40.
[16] Peleg, M., Shahar, Y., Quaglini, S., Broens, T., Budasu, R., Fung, N., Fux, A., Garcia-Saez, G., Goldstein, A., Gonzalez-Ferrer, A., Hermens, H., Hernando, M. E., Jones, V., Klebanov, G., Klimov, D., Knoppel, D., Larburu, N., Marcos, C., Martinez-Sarriegul, I., Napolitano, C., Pallas, A., Palomares, A., Parimbelli, E., Pons, B., Rigla, M., Sacchi, L., ShalomH, E., Soffer, P. & Van Schooten, B. 2017, Assessment of a personalized and distributed patient guidance system. *Int J Med Inform,* 101**,** 108-130.
[17] Pfiffner, P. B., Pinyol, I., Natter, M. D. & Mandl, K. D. 2016, C3-PRO: Connecting ResearchKit to the health system using i2b2 and FHIR. *PLoS ONE,* 11.
[18] Rubio, O. J., Trigo, J. D., Alesanco, A., Serrano, L. & García, J. 2016, Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility. *Journal of Biomedical Informatics,* 60**,** 270-285.
[19] Song, Y.-T. & Qiu, T. 2016, Standard based personal mobile health record system. *ACM IMCOM 2016: Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication,* 0.
[20] Tachakra, S., Wang, X. H., Istepanian, R. S. & Song, Y. H. 2003, Mobile e-health: the unwired evolution of telemedicine. *Telemed J E Health,* 9**,** 247-57.
[21] Young, D. R., Bauck, A., Go, A. S., Corley, D. A., Morales, L. S., Mcglynn, E. A., Lieu, T. A., Durham, M. L., Laws, R., Chen, J., Feigelson, H. S., Nelson, A. F., Davidson, A. J. & Kahn, M. G. 2014, Developing a data infrastructure for a learning health system: the PORTAL network. *Journal of the American Medical Informatics Association : JAMIA,* 21**,** 596-601.

Acknowledgement

This work is supported by the Research Council of Norway (through the project "Full Flow of Health Data Between Patients and Health Care Systems", project number 247974/O70) and the Norwegian Centre for E-health Research through the Data Exchange project, a collaborative project with The Norwegian Directorate of eHealth .

Ref.	Data Sou. *	Data Coll. **	Data Type ***	Interoperability	Security Privacy	System
(Song and Qiu, 2016)	App	Aut.	S U	CDA, SNOMED, ICD-10, DICOM		Personal Mobile Health Record (PMHR)
(Rubio et al., 2016)	App, Man			ISO11073, X73PHD, HL7	Twofish, RSA2048, SHA512, RIPEMD256, ECDSA256	
(Pfiffner et al., 2016)	App, Man	Aut.	S	FHIR	OAuth2, AES 256, PKCS7, UUID, Explicit consent	End-to-End Research (ResearchKit, HealthKit i2b2)
(Park et al., 2016)	App, Man, Sen	Aut.	S	Continua-based	Continua-based	Self-management Mobile Personal Health Record
(Kumar et al., 2016)	App, Man, Sen	Aut. Man.	S	CCD-HealthKit	Explicit consent	End-to-End (Epic HER, HealthKit,Share2)
(Horder n, 2016)	App, Man, Sen, Cl				Transparency disclosure, Explicit consent, data access	
(Marceglia et al., 2015)	App	Man.	S	CDA2, SNOMED, LOINC	De-identified data, XPHR	End-to-End POC (OpenMRS, IOS app)
(Leijdekkers and Gay, 2015)	App, Man, Sen	Aut.	S	HL7 (CDD-HealthVault)	OAuth2	Android App (Healthvault, Google fit, Fitbit, Jawbone, Withings)
(Gay and Leijdekkers, 2015)	App, Man, Sen	Aut.	S	HL7 (CCD-HealthVault)	OAuth2	Android App (Healthvault, Google fit, Fitbit, Jawbone, Withings)
(Young et al., 2014)	Ehr	Aut.	U	CESR CDM, SNOMED, ICD		Portal network member

Table 1. Papers included in the review ordered by date.
*Patient-data source: App=mobile applications, Man=Managers/aggregators, Sen=Sensors, Ehr=EHR, Cl=Cloud. **Data collection: Aut=Automatic, Man=Manual. ***Patient data type: U=Unstructured, S=Structured. Empty field means the subject was not described in the paper.