Legal and Regulatory Considerations Associated with Use of Patient-Generated Health Data from Social Media and Mobile Health (mHealth) Devices

C. Petersen[1]; P. DeMuro[2,3]

[1]Mayo Clinic, Rochester, Minnesota, USA; [2]Department of Medical Informatics and Clinical Epidemiology, Oregon Health & Science University, Portland, Oregon, USA; [3]Schwabe, Williamson & Wyatt, Seattle, Washington, USA

Summary

Patient-generated health data are coming into broader use across the health care spectrum and hold great promise as a means to improve care and health outcomes. At the same time, rapid evolution in the social media and mobile health (mHealth) market has promoted an environment in which creation and transmission of personal health information is easy, quick, and appealing to patients. However, adoption of social media and mHealth by providers is hampered by legal and regulatory concerns with regard to data ownership and data use. This article defines common forms of patient-generated health data (PGHD) and describes how PGHD is used in clinical settings. It explores issues related to protection of personal health information, including that of children and adolescents, data security, and other potential barriers such as physician licensure. It also discusses regulatory and legal considerations providers and patients should consider before using social media and mobile health apps.

Correspondence to:

Carolyn Petersen, MS, MBI
Mayo Clinic
Global Business Solutions
200 First St. SW
Rochester, MN 55905
Email: petersen.carolyn@mayo.edu

1. Introduction

Patient-generated health data (PGHD), also known as patient-generated health information, has been defined as health-related data created, recorded, gathered or inferred by or from patients or their designees (care partners or those who assist them) to help address a health concern [1]. It differs from data generated in clinical settings and during interactions with care providers in that patients capture or record PGHD and determine with whom it will be shared. Patients' control over information about them differentiates patient-generated health data from patient-directed health information, which is data that can be shared across systems without input from patients and their caregivers [2].

Patient-generated health data emanate from multiple sources, including patient-reported outcomes (PROs), patient-powered patient registries (PPRs), patient-powered research networks (PPRNs), patient portals, remote sensors, smart wearable devices, social media, mobile health (mHealth) apps, and others. Patient-reported outcomes, also known as patient-reported outcome measures (PROMs), are used in research and clinical settings to assess how patients perceive their health status. Patient-powered registries are collections of standardized information about a group of patients who share a condition or experience [3]. PPRs use existing data or data contributed and managed by patients to assess treatment effectiveness, adverse effects, and similar considerations that are of interest to patients. Patient-powered research networks bring together multiple registries in a shared infrastructure [3]. Patient portals include Web- or mobile device-based structures through which patients can access provider-created and -maintained information about them and their health. Smart wearable devices transmit personal data such as heart rate and activity level to an external source for analysis.

Patient-reported outcomes have been reported since the late 1980s [4, 5]. They frequently have been used in clinical trials to measure symptoms, quality of life, and other qualities or states that are not captured by clinical endpoints such as disease-free survival and response rate. PROs differ from PGHD in that PROs describe a condition or status at a particular point (e.g., depression 180 days postsurgery), whereas PGHD may be single data points (e.g., minutes of rapid eye movement sleep during a particular night) that must be analyzed along with additional PGHD to describe a condition or status.

Though the collection and use of patient-generated information is intuitive to experienced patients, inclusion of such data represents a shift in the way medicine has been practiced [6]. However, patient experience based-outcomes may be of equal interest to patients who may need to evaluate and choose among multiple treatment options when no therapy offers a clear advantage in survival, as is the case with many cancers [7]. Taking an active role in the collection and management of data about one's health status increases patient activation, which is strongly related to better health outcomes in multiple conditions [8, 9].

Despite the significant potential benefits to outcomes and patient satisfaction that may accrue through the leveraging of PGHD in clinical care, data ownership remains a barrier to greater use of PGHD in some circumstances. This article reviews the data ownership and regulation issues with regard to PGHD created and/or distributed via social media and mobile health applications.

2. Benefits from use of PGHD

Use of PGHD facilitates the realization of numerous desirable outcomes and events. For example, the National Institutes of Health asthma guidelines recommend the use of patient-reported outcomes in assessment of asthma control [10]. The delivery of customized care plans and acquisition of PROs during hospitalization after cardiac surgery has been shown to predict length of hospital stay and health status at discharge [11]. Similarly, length of stay has been associated with a patient-generated subjective global assessment of nutritional status in adults who had undergone an appendectomy [12]. The value of patient-generated information for assessing patients' functional status has been recognized for many years [13].

The use of PGHD also can facilitate improvements in the health care system. Analysis of data submitted by members of the patient network PatientsLikeMe about their use of lithium carbonate

as a treatment for amyotrophic lateral sclerosis was similar to analysis of clinical trial data, suggesting that PGHD may have a role in drug discovery and development [14, 15]. Combining reports from the US Food & Drug Administration's (FDA) adverse event reporting system with PGHD collected from Internet search logs improved the accuracy of adverse drug reaction detection by 19% over either approach used alone [16]. PROs gathered electronically (ePROs) and archived in a central institutional system have a prominent role in the achievement of a rapid learning cancer care system [17].

Beyond the advantages to patients that accrue through the use of patient-generated information, public policy supports greater use of PGHD in a more patient-centered learning health care environment. The Office of the National Coordinator for Health Information Technology has indicated that bringing patient-reported data into certified electronic health records (EHRs) is a high priority and is expected to include requirements to stimulate greater patient engagement in stage 3 of the meaningful use electronic health record incentive program [18, 19]. In 2009 FDA issued a guidance describing how it evaluates PRO instruments that are collected to support labeling claims in medical product development [20]. In addition, FDA has acknowledged the need to use patient-generated information in such as that shared via social media in pharmacovigilance [21].

Finally, patients themselves have described the value they derive from taking an active role in providing information used in making care decisions and improving the health care system. Patients' descriptions of their engagement in adverse drug reaction reporting within a formal pharmacovigilance infrastructure, cancer-related symptom reporting and management, and use of PROs to guide the care they receive illustrate the difference patients can make in their own health outcomes when PGHD is considered in conjunction with other clinical evidence [22–25]. Patients and providers see the same clinical encounter from very different perspectives, and the use of patient-generated information in the course of care can close that gap.

3. Social media and mobile health

Although social media and mobile health (mHealth) address separate purposes, they are often thought of in tandem because social media platforms such as Twitter lend themselves to distribution of PGHD and mHealth apps frequently are built to transmit PGHD to health care providers or others (e.g., online fitness sites) for analysis. Some operational and legal issues affect both social media and mHealth, while others are relevant to just one.

FDA defines mobile apps as software programs that run on smartphones and other mobile communication devices, accessories that attach to a smartphone or other mobile communications devices, or a combination of accessories and software [26]. The agency defines mobile medical apps as "medical devices that are mobile apps, meet the definition of a medical device, and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device" [26]. Mobile medical apps generally serve one or more of several purposes, including treatment and disease management; data collection and disease surveillance; health support systems; health promotion and disease prevention; communication between patients and health care providers or among providers; and medical education [27]. Although there is great variety of format and function among mobile medical apps, mHealth most often involves text messaging, for example between patient and clinician [27].

Patients' and providers' use of social media and mHealth apps provide a framework for assessing the role mHealth can play in medicine and as a source of PGHD. Physicians use social media primarily for personal use (60%), though accessing health care news (21%), communicating with peers (18%), marketing the practice (11%), and communicating to patients (4%) are also practiced [28]. Among physicians who choose not to use social media, concerns about patient privacy (52%), lack of time (51%), concerns about liability (42%), the belief that social media has little professional value (40%), and lack of familiarity (23%) are cited most frequently. In 2014, two-thirds of physicians surveyed reported using a mobile app to check medication interactions, diagnose a condition, access electronic health records (EHRs), check results, create clinical notes, and prescribe electronically, and more than a third of US physicians recommended their patients use health apps [29, 30].

Social media and mHealth use among consumers and patients is more difficult to track because of the broad range of platforms and mobile apps available and the integration of platforms and apps into users' personal (as opposed to professional) lives. Many people use multiple platforms and apps, which makes it possible for individuals to be counted multiple times. About 46 million unique users in the US accessed fitness and health apps from a smartphone in January 2014, an 18% increase from January 2013 [31]. Worldwide, three million patients used connected home medical monitoring devices for remote monitoring by professionals at the end of 2013, and the number of patients using such devices is expected to grow to 19.1 million by 2018 [32].

4. Growth of social media and mHealth

Growth in mobile health device use and services via apps and traditional medical devices (e.g., Internet-connected monitoring equipment) has been projected for some time. Besides the obvious popularity of consumer apps, other factors could drive growth in mHealth, including new technologies, greater interest by patients and providers in sharing information, financial and other incentives to exchange PGHD, and documentation of improved outcomes or lower health care costs with use of mHealth devices [1].

Growth estimates by user market size provide a way to quantify the current and future mHealth environment:

- A market of 15 million users of app-enabled mHealth and mobile-fitness hardware devices in 2013 is projected to grow to more than 96 million in 2018 [33]
- By 2018, 50% of an estimated 3.4 billion smartphone and tablet users will have downloaded mHealth apps [34]
- Three million patients will be monitored remotely by 2016 [35]
- One-third of smartphone owners – 48.5 million people – in the United States used health/fitness apps in January 2014, an 18% increase from January 2013 [36]
- 27% of US households own and use at least one connected device health device such as a piece of exercise equipment, and an additional 13% of households intend to purchase such a device within a year [37]

Estimates of the financial value of the mHealth market provide yet another way to regard mHealth's potential:

- The global mHealth market was valued at $1.95 billion in 2012 and is projected to reach $49 billion by 2020 [38]
- The global mHealth monitoring and diagnostic market was valued at $650 million in 2012, and is projected to reach $8 billion in 2019 [39]
- The global connected devices market was valued at $5.3 billion in 2013 and is projected to reach $16.4 billion by 2018 [40]
- The global wireless EHR market was valued at $11.2 billion in 2013 and is projected to reach $23.5 billion in 2018 [41]
- Nearly 100 million wearable remote patient monitoring devices, such as continuous glucose monitors, are projected to ship through 2019 [42]

5. Legal issues and PGHD

Social media tools such as Facebook, Twitter, LinkedIn, and others have created abundant opportunities for patients and their families and friends to share personal information related to one's own health and the health of others. Mobile devices such as smartphones and tablets facilitate both the publication of personal health information via social media and the creation of personal health information via wearable technology, sensors, and other devices.

5.1 Social media data ownership

It is generally thought that the person who generates data owns the data until that person posts such data on a social media site, whether doing so from a laptop or through a mobile device. At that time, most social media sites take the position that the data is theirs and, often, that they can use it as they wish. The terms and conditions a user must accept prior to joining such a site generally provide that the social media site owns the data, though the content author may retain some rights. For example, the Terms of Service of Twitter note, "You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)." [43] Twitter's Terms of Service identify the rights that Twitter users transfer to the service on creation of content, but do not address the rights of providers and health care organizations wishing to incorporate patient data distributed over Twitter into patients' EHRs, which could pose a barrier for providers.

Many complications can be created by a social media site owning an individual's data. In 2012 the European Union (EU) introduced the right to be forgotten [44], which has since been implemented through such action as a requirement that the search engine Google remove links to personal information on the request of the individual [45, 46]. Social media posts containing PGHD that can be accessed via search engines will likely be covered under the right to be forgotten, potentially creating complications for providers and health care organizations seeking to include PGHD in EHRs. If providers and health care organizations set up processes to download PGHD from the Internet into EHRs and provider-hosted PHRs (e.g., via an automated Web search), they should implement a process for handling patient requests for removal of PGHD from health records, since patients' information removal requests to search engines are unlikely to affect PGHD in health records. Processes for removal of PGHD emanating from sources that are not Web-searchable, such as patient-powered networks or data registries, will need to take into account the terms of service of these sources.

What might become of personal information owned by a social media site? Consider the example of a social media site to which individuals who have a particular condition post information about their condition, the drugs they are taking, the side effects they are experiencing, their progress in managing their condition, and even the availability of and participation in clinical trials. It is advisable for individuals posting personal information on such a site and participating in it to know who owns the site because that entity might well own the data of all participating on the site. Some important considerations include:

- Is the site owned by a nonprofit academic institution, a pharmaceutical or medical device company, a single provider, an entrepreneur, or a different entity?
- Are certain privacy and security issues implicated or have they been waived by the mere posting of the information by the individual? Will any further consent processes be needed beyond the clicking of "Yes" to the Terms and Conditions of the site?
- What does the owner of the data intend to do with it today, tomorrow and in the future?
- Will the data primarily be used to facilitate the care and treatment of those posting to the site? Will the data be sold to others who might monetize it?
- Will the site be used as a venue from which to recruit individuals for clinical trials?
- If clinical trials are conducted in conjunction with the site, and value is generated by same, who owns that value?

Any of these uses can result in a plethora of legal issues and considerations, including whether the site owner may use the data as he/she desired.

It is also possible that providers may use a public social media site in the diagnosis and/or treatment of patients, as has been done with Facebook for the diagnosis of common skin conditions and rare congenital conditions that require complex care [47]. In this and similar cases, the social media site operator as well as the provider and patient have an ownership stake in the data. The social media site's Terms of Service will determine how the social media site may use the data.

How might such social media sites interface with an individual's EHR or personal health record (PHR)? Although a topic of debate, in the United States, it is generally accepted that an individual's

medical record is owned by the provider who retains the record, not the individual whose medical information resides in the record [48]. As providers move to EHRs, the location of information from an individual's EHR might be in more disparate locations, but providers still take the position that they own a patient's medical record. This ownership, however, does not take all rights away from patients as they are still covered by privacy protections included in the Health Insurance Portability and Accountability Act of 1996 [49]. As more and more information from different places is put in that EHR, e.g. treatment from health system one on day one, treatment from a free-standing urgent care clinic on day two, and treatment from health system two on day three, ownership issues may become more complicated. However, in the context of a patient's PHR, it is generally thought that the patient owns the PHR. Although PHRs are not yet ubiquitous, they can hold promise for the future if patients truly update and correct their health care and treatment information.

5.2 mHealth data ownership

The area of mHealth might be viewed as connected to social media because individuals often access or post on a social media site through a mobile device. mHealth devices might well facilitate what is on such social media sites. The device might be one personally owned by an individual – so-called BYOD, or Bring Your Own Device – one owned by an employer, family member, or friend, or one given to a patient by a health care provider.

Ownership of an mHealth device with an individual's personal health information can raise numerous legal issues, not the least of which are those concerning privacy and security. As noted previously, providers and patients might use such devices in the diagnosis of conditions, the checking of results, and in the provision of care. Certain of this information may be posted voluntarily or automatically to a particular site. The latter instance could include situations in which a provider or health system monitors an individual's chronic condition. An examination of the 600 most commonly used mHealth apps revealed that only 30.5% had a privacy policy, and two-thirds of these privacy policies focused on a developer Web page, developer services, or subjects other than the app [50].

Information input by an individual into a mobile device generally starts out as that individual's data similar to information individuals enter into a personal computer. Such information may be input by virtue of entering data or by sensor or other means that convey data about an individual, such as a blood glucose measurement, to a device. Once the data is entered into the mHealth device, it could be transmitted elsewhere. If it is then transmitted, where it is transmitted can affect its ownership. For example, if the data are transmitted into a patient's medical record, both the owner of the medical record (e.g., the clinician or the hospital hosting the medical record) and the individual transmitting the data now have an ownership stake in the information transmitted by the mHealth device. If the sender transmits the data to his/her personal health record, the sender may still be the owner, if he or she owns the PHR.

5.3 mHealth regulation

FDA regulates certain medical devices and also certain mobile medical apps. On September 25, 2013, it issued a Final Guidance that defines "mobile medical app," as a mobile app that (1) meets the definition of a "device" in the Federal Food, Drug and Cosmetic Act and (2) is intended to be used as an accessory to a "regulated medical device' or to transform a platform into a "regulated medical device [51]." The Guidance grouped mobile medical apps into three categories: 1) apps that are actively regulated, (e.g., a mobile medical app that monitors the patient's HbA1c and calculates the amount of insulin needed based on the patient's condition, age, weight, etc.); 2) apps that are subject to enforcement discretion, (e.g., a mobile medical app that provides a patient an alert as to when to take his or her medications); and 3) those that are not considered devices and thus are not regulated (e.g., a mobile medical app that merely provides general health care information available on the Internet, not directed to a specific patient).

The FDA guidance addresses data security because patients and other users may experience severe consequences should the device lack adequate data protection or be hacked. The guidance does not address the protection of privacy. Rather, privacy is protected by the Health Insurance Portabil-

ity and Accountability Act (HIPAA), where applicable. When patients' health information is in the possession of health providers, health plans, business associates, or other covered entities, it is protected under HIPAA; when it is transmitted among individuals or organizations that are not covered entities under HIPAA, it is not protected. Accordingly, health information transmitted via a mobile device by a covered entity is protected under HIPAA privacy and security rules. However, this same information transmitted via a non-covered entity under HIPAA is not protected [52]. HIPAA also does not cover information on an individual's mobile device.

PGHD is merely data of the patient if a patient checks his or her HbA1c with a mobile device. If, however, he or she uses the device to transmit that information to his or her clinician for the purpose of monitoring that person's care and the information becomes part of the patient's EHR, the PGHD then falls under HIPAA [53].

Questions related to provider licensure pose another potential barrier to the routine use of mHealth. When a patient has his or her radiograph read, many current US state laws require that it be read by a physician licensed in the state where the patient is located and had the radiograph. PGHD can raise special issues. For example, if a patient lives in New York and has an mHealth device that continues to monitor certain aspects of his or her health and the patient crosses three states and then travels into the EU, does the patient's physician need to be licensed in each of the other three states and in the applicable country in the EU when the data is transmitted from that state or country in the EU? Within the United States, most states require that the out-of-state physician receive an unrestricted license in the state in which the initial patient interaction occurred [54, 55]. Some states issue a telemedicine license to facilitate practice across state lines when the physician holds an unrestricted license in another state [56]. In the radiograph situation, the imaging physician is reading the radiograph at one point in time and billing for that service. With the monitoring of an individual's health information continuously, the clinician may be being paid to manage the patient's condition or his or her overall care.

The special privacy and confidentiality issues, such as those involving family planning services and treatment for sexually transmitted diseases, associated with teenagers and their treatment can raise important mHealth implications. It is important that vendors and health care systems coordinate their efforts to minimize these issues [57]. Pediatric hospitals need to be sensitive to the special issues raised in the use of PHRs by their patients and families, such as what might be added to a PHR, how, and by whom, that can be occasioned by the link between a patient's EHR and PHR. The interoperability between the EHR and PHR must be able to facilitate the free flow of information consistent not only with applicable law and regulations but also within the context of social, societal, and organizational considerations [58].

The Federal Trade Commission (FTC) is not hesitant to file complaints against companies that it believes fail to reasonably protect the security of consumers' personal data, including medical information. In August 2013 FTC filed a complaint against LabMD, Inc., alleging that the medical testing laboratory exposed the personal medical information of more than 9,000 consumers by placing the information on a peer-to-peer file-sharing network [59]. The filing followed the discovery of the personal information of several hundred consumers who used LabMD's services in the possession of identity thieves. In this case, as in an earlier case against a medical transcription firm that exposed personal medical information on the public Internet, FTC is acting to enforce HIPAA's security requirements [60].

FTC also regulates misleading claims. If in the sale or distribution of a mobile medical app or device one makes claims about what the device can do, FTC can bring an action to make the individual or entity cease and desist from making such claims. In 2013 FTC published a written guidance and a short video for mobile app developers that offer advice on creating apps that protect users' privacy and comply with truth-in-advertising principles [61, 62].

Future directions

Full realization of the potential for patient-generated health data to improve patient outcomes on a large scale and support the transformation to a learning health care system requires further evolution in both technical and regulatory areas. As with other forms of health information technology,

the development and use of standards for data representation and transmission is a key factor needed to create the secure environment necessary for social media- and mHealth-based applications to flourish. It is also critical that mobile app developers become more transparent about their data ownership and data use policies so that patients, in conjunction with their providers, can make informed choices about when and how to create and transmit patient-generated health data. Such transparency will make possible the discussions about patient expectations and provider concerns needed for both parties to benefit from use of PGHD.

Clinical Relevance Statement

Use of social media and mHealth for the collection and transmission of patient-generated health data is becoming more common. Understanding legal and regulatory issues related to data ownership and data use allows clinicians to align their needs and interests with those of their patients, thereby facilitating informed decision making about use of data-sharing technologies.

Conflict of Interest

The authors declare that they have no conflicts of interest in the research.

Human Subjects Protections

Human and animal subjects were not included in the development of this work.

Acknowledgements

References

1. Shapiro M, Johnston D, Wald J, Mon D. Patient-generated health data (white paper). 2012 Apr [cited 2014 Sep 1]. Available from https://www.rti.org/pubs/patientgeneratedhealthdata.pdf.
2. National eHealth Collaborative. Patient-generated health information technical expert panel final report. 2013 Dec [cited 2014 Sep 1]. Available from http://www.healthit.gov/sites/default/files/pghi_tep_finalreport121713.pdf.
3. Agency for Healthcare Research and Quality. Engaging patients in information sharing and data collection: the role of patient-powered registries and research networks. AHRQ publication AHRQ 13-EHC124-EF. 2013 Sep [cited 2014 Sep 1]. Available from http://www.ncbi.nlm.nih.gov/books/NBK164513/pdf/TOC.pdf.
4. Von Korff MR, Howard JA, Truelove EL, Sommers E, Wagner EH, Dworkin S. Temporomandibular disorders. Variation in clinical practice. Med Care 1988; 26(3): 307–314.
5. Stewart AL, Greenfield S, Hays RD, Wells K, Rogers WH, Berry SD, McGlynn EA, Ware JE Jr. Functional status and well-being of patients with chronic conditions. Results from the Medical Outcomes Study. JAMA 1989; 262(7): 907–913.
6. Richards T, Montori VM, Godlee F, Lapsey P, Paul D. Let the patient revolution begin. BMJ 2013; 346 : f2614.
7. Basch E. Toward patient-centered drug development in oncology. New Engl J Med 2013; 369(5): 397–400.
8. Greene J, Hibbard JH. Why does patient activation matter? An examination of the relationships between patient activation and health-related outcomes. J Gen Intern Med 2012; 27(5): 520–526.
9. Dentzer S. Rx for the 'blockbuster drug' of patient engagement. Health Aff (Millwood) 2013; 32(2): 202.
10. Shen J, Johnston M, Hays RD. Asthma outcome measures. Expert Rev Pharmacoecon Outcomes Res 2011; 11(4): 447-453.
11. Cook DJ, Manning DM, Holland DE, Prinsen SK, Rudzik SD, Roger VL, Deschamps C. Patient engagement and reported outcomes in surgical recovery: effectiveness of an e-health platform. J Am Coll Surg 2013; 217: 648–655.
12. Huang TH, Chi CC, Liu CH, Chang CC, Kuo LM, Hsieh CC. Nutritional status assessed by scored patient-generated subjective global assessment associated with length of hospital stay in adult patients receiving an appendectomy. Biomed J 2014; 37(2): 71–77.
13. Bierman AS. Functional status: the sixth vital sign. J Gen Intern Med 2001; 16(11): 785–786.
14. Wicks P, Vaughan TE, Massagli MP, Heywood J. Accelerated clinical discovery using self-reported patient data collected online and a patient-matching algorithm. Nat Biotechnol 2011; 29(5): 411–414.
15. Harpaz R, DuMouchel W, Shah NH, Madigan D, Ryan P, Friedman C. Novel data-mining methodologies for adverse drug event discovery and analysis. Clin Pharmacol Ther 2012; 91(6): 1010–1021.
16. White RW, Harpaz R, Shah NH, DuMouchel W, Horvitz Z. Toward enhanced pharmacovigilance using patient-generated data on the Internet. Clin Pharmacol Ther 2014; 96(2): 239–246.
17. Abernathy AP, Ahmad A, Zafar Y, Wheeler JL, Reese JB, Lyerly HK. Electronic patient-reported data capture as a foundation of rapid learning cancer care. Med Care 2010; 48(6 Suppl.): S32-S38.
18. Terry K. Patient-reported functional status data may soon be included in EHRs. iHealthbeat 2013 Nov 25 [cited 2014 Sep 7]. Available from http://www.ihealthbeat.org/insight/2013/patientreported-functional-status-data-may-soon-be-included-in-ehrs
19. Office of the National Coordinator for Health Information Technology. Request for comment regarding the stage 3 definition of meaningful use of electronic health records (EHRs). 2012 Nov [cited 2014 Sep 7]. Available from http://www.healthit.gov/sites/default/files/hitpc_stage3_rfc_final.pdf.
20. Food and Drug Administration. Guidance for industry: patient-reported outcome measures: use in medical product development to support labeling claims. 2009 Dec [cited 2014 Sep 1]. Available from http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm193282.pdf.
21. FDA Science Board Subcommittee. Review of the FDA/CDER pharmacovigilance program. 2011 May [cited 2014 Sep 1]. Available from http://www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/ScienceBoardtotheFoodandDrugAdministration/UCM276888.pdf.
22. Anderson C, Krska J, Murphy E, Avery A on behalf of the Yellow Card Study Collaboration. The importance of direct patient reporting of suspected adverse drug reactions: a patient perspective. Br J Clin Pharmacol 2011; 72(5): 806–822.
23. van Hunsel F, van der Welle C, Passier A, van Puijenbroek E, van Grootheest K. Motives for reporting adverse drug reactions by patient-reporters in the Netherlands. Eur J Clin Pharmacol 2010; 66(11): 1143–1150.

24. Abernathy AP, Herndon JE, Wheeler JL, Day JM, Hood L, Patwardhan M, Shaw H, Lyerly HK. Feasibility and acceptability to patients of a longitudinal system for evaluating cancer-related symptoms and quality of life: pilot study of an e/tablet data-collection system in academic oncology. J Pain Symptom Manage 2009; 37(6): 1027–1038.

25. Chauhan C. The perception of perception. J Clin Oncol 2007; 25(16): 2329–2330.

26. Food and Drug Administration. Mobile medical applications. 2014 Jun 4 [cited 2014 Nov 22]. Available from http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/Mobile MedicalApplications/default.htm.

27. Nhavoto JA, Grönlund A. Mobile technologies and geographic information systems to improve health care systems: a literature review. JMIR Mhealth Uhealth 2014; 2(2): e21.

28. MedData Group. Physician adoption of social media; 2014 Q2 [cited 2014 Sept 1]. Available from http://www.meddatagroup.com/wp-content/uploads/MedDataGroup-Physician-Adoption-of-Social-Media-Q22014.pdf.

29. MedData Group. Physician perceptions of mobile & connected health; 2014 Q2 [cited 2014 Sept 1]. Available from http://ci28.actonsoftware.com/acton/attachment/3366/f-0252/1/-/-/-/-/mediareportnonmarket-ing.pdf.

30. Manhattan Research. Stethoscopes and smartphones: physicians turn to digital tools to boost patient outcomes [Internet]. Manhattan Research's Taking the Pulse® U.S. 2014 Study; 2014 May 29 [cited 2014 Sept 1]. Available from http://www.manhattanresearch.com/News-and-Events/Press-Releases/Digital-Tools-to-Boost-Patient-052914.

31. Nielsen. Hacking health: how consumers use smartphones and wearable tech to track their health. Nielsen's Connected Life Report; 2014 Apr 16 [cited 2014 Sept 1]. Available from http://www.nielsen.com/us/en/insights/news/2014/hacking-health-how-consumers-use-smartphones-and-wearable-tech-to-track-their-health.html.

32. Berg Insight. mHealth and home monitoring, 6th edition: executive summary. 2014 June; [cited 2014 Sept 1]. Available from http://www.berginsight.com/ReportPDF/Summary/bi-mhealth6-sum.pdf.

33. Juniper Research Ltd. Smartphone-based fitness and mHealth device users to approach 100 million by 2018, finds Juniper Research. 2013 Sep 11 [cited 2014 Sep 13]. Available from http://www.juniperresearch.com/viewpressrelease.php?id=591&pr=399.

34. research2guidance. Mobile health market report 2013–2017: the commercialization of mHealth applications (vol.3). 2013 Mar 4 [cited 2014 Sep 13]. Available from http://www.research2guidance.com/shop/index.php/downloadable/download/sample/sample_id/262/.

35. Juniper Research Ltd. mHealth users of remote health monitoring to reach 3 million by 2016: smartphones play leading role. 2012 Feb 2 [cited 2014 Sep 13]. Available from http://www.juniperresearch.com/view pressrelease.php?pr=285.

36. Nielsen. Hacking health: how consumers use smartphones and wearable tech to track their health. 2014 Apr 16 [cited 2014 Sep 13]. Available from http://www.nielsen.com/us/en/insights/news/2014/hacking-health-how-consumers-use-smartphones-and-wearable-tech-to-track-their-health.html.

37. Parks Associates. Nearly 30% of U.S. broadband households own and use a connected health device. 2014 Sep 4 [cited 2014 Sep 13]. Available from http://www.parksassociates.com/blog/article/chs-2014-pr17.

38. Grand View Research. mHealth market analysis and segment forecasts to 2020. 2014 Feb [cited 2014 Sep 13]. Available from http://www.grandviewresearch.com/industry-analysis/mhealth-market.

39. Transparency Market Research. mHealth monitoring and diagnostic medical devices market (focus on medical devices with in-built plug-ins for connectivity with devices like smartphones and tables) global industry analysis, size, share, growth, trends and forecast, 2013–2019. 2014 Apr 28 [cited 2014 Sep 13]. Available from http://www.transparencymarketresearch.com/mHealth-monitoring-diagnostic-medical-devices.html.

40. MarketsandMarkets, Mobile health apps & solutions market by connected devices (cardiac monitoring, diabetes management devices), health apps (exercise, weight loss, women's health, sleep and meditation), medical apps (medical reference) – global trends & forecast to 2018. 2013 Sep [cited 2014 Sep 13]. Available from http://www.marketsandmarkets.com/Market-Reports/mhealth-apps-and-solutions-market-1232.html.

41. BCC Research LLC. Wireless electronic health records: technologies and global markets. 2014 Jan [cited 2014 Sep 13]. Available from http://www.bccresearch.com/market-research/healthcare/wireless-electronic-health-records-hlc147a.html.

42. ABI Research Inc. Foundations emerge for a revolution in remote patient monitoring. 2014 Sep 4 [cited 2014 Sep 13]. Available from https://www.abiresearch.com/press/foundations-emerge-for-a-revolution-in-remote-pati.

43. Twitter. Terms of service. 2014 Sep 8 [cited 21 Nov 2014]. Available from https://twitter.com/tos.

44. European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012 Jan 25 [cited 2014 Nov 22]. Available from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

45. Court of Justice of the European Union. An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. 2014 May 13 [cited 2014 Nov 22]. Available from http://curia.europa.eu/jcms/upload/docs/application/pdf/2014–05/cp140070en.pdf.

46. Lowe R. Right to be forgotten sparks fresh debate over privacy and freedom of expression. 2014 Jun 20 [cited 2014 Sep 1]. Available from http://www.ibanet.org/Article/Detail.aspx?ArticleUid=0d7cae7f-89ca-42da-b744–0a6771d5dbcf.

47. Garcia-Romero MT, Prado F, Dominguez-Cherit J, Hojyo-Tomomka MT, Arenas R. Teledermatology via a social networking web site: a pilot study between a general hospital and a rural clinic. Telemed J E Health 2011; 17(8): 652–655.

48. Brodnik MS, Rinehart-Thompson LA, Reynolds RB (eds). Fundamentals of law for health informatics and information management, 2nd ed. Chicago, IL; Chicago, IL: American Health Information Management Association; 2012.

49. US Department of Health & Human Services. OCR privacy brief: summary of the HIPAA privacy rule. 2003 May [cited 2014 Nov 21]. Available from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

50. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. J Am Med Inform Assoc Published Online First: 2014 Sep 8 doi:10.1136/amiajnl-2013–002605.

51. Food and Drug Administration. Mobile medical applications: guidance for industry and food and drug administration staff. 2013 Sep 25 [cited 2014 Sep 7]. Available from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

52. Office of the National Coordinator for Health Information Technology. Do you need to comply with HIPAA if you are using a mobile device? 2013 Jan 15 [cited 2014 Nov 21]. Available from http://www.healthit.gov/providers-professionals/faqs/do-you-need-comply-hipaa-if-you-are-using-mobile-device.

53. Fisher M. Will the hippo swallow the apple? HITECH Answers 2014 Jun 12 [cited 2014 Nov 22]. Available from http://www.hitechanswers.net/apples-health-app-healthkit-hipaa/.

54. American College of Radiology. Teleradiology (state level). Undated [cited 2014 Nov 22]. Available from http://www.acr.org/Advocacy/State-Local-Relations/Legislative-Issues/Teleradiology.

55. American College of Radiology. Teleradiology licensing requirements by state. Undated [cited 2014 Nov 22]. Available from http://www.acr.org/Advocacy/State-Local-Relations/Legislative-Issues/Teleradiology/Teleradiology-Licensing-Requirements-by-State.

56. Coffey JE. State laws vary in regulation of teleradiology execution. 2001 Dec 1 [cited 2014 Nov 22]. Available from http://www.diagnosticimaging.com/articles/state-laws-vary-regulation-teleradiology-execution.

57. Anoshiravani A, Gaskin GL, Groshek MR, Kuelbs C, Longhurst CA. Special requirements for electronic medical records in adolescent medicine. J Adolesc Health 2012 Nov; 51(5): 409–414.

58. Anoshiravani A, Gaskin G, Kopetsky E, Sandborg C, Longhurst CA. Implementing an interoperable personal health record in pediatrics: lessons learned at an academic children's hospital. J Particip Med 2011; 3: e30.

59. Federal Trade Commission. LabMD, Inc., in the matter of. 2014 Aug 11 [cited Sep 19]. Available from http://www.ftc.gov/enforcement/cases-proceedings/102–3099/labmd-inc-matter.

60. Federal Trade Commission. Provider of medical transcript services settles FTC charges that it failed to adequately protect consumers' personal information. 2014 Jan 31 [cited 2014 Sep 7]. Available from http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

61. Federal Trade Commission. Mobile privacy disclosures: building trust through transparency. 2013 February [cited 2014 Sep 7]. Available from http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

62. Federal Trade Commission. FTC announces video with tips for mobile app developers. 2013 March 13 [cited 2014 Sep 7]. Available from http://www.ftc.gov/news-events/press-releases/2013/03/ftc-announces-video-tips-mobile-app-developers.