Journal of Information Systems and Technology Management – Jistem USP
Vol. 16, 2019, e201916003
ISSN online: 1807-1775
DOI: 10.4301/S1807-1775201916003

UNDERSTANDING THE ORGANIZATIONAL BARRIERS OF PROMOTING ELECTRONIC DELIVERY OPTIONS IN THE UNITED STATES HEALTHCARE SYSTEM: AN INSURER'S PERSPECTIVE

Danielle A. O'Leary https://orcid.org/0000-0001-5803-7904
Joan M. Kiel https://orcid.org/0000-0002-9851-3319

Duquesne University, Pittsburgh, PA, USA

ABSTRACT

Consumer-driven technologies are rapidly transforming how industries conduct business both internally and externally. From online banking to retail, the broad adoption of smart devices, internet access, and wearables amongst consumers has shifted the way enterprises develop software and conduct information technology (IT) operations. Although successful adoption of consumer-driven technologies is a reality for many industries, the healthcare platform is lagging. The promotion and adoption of online patient engagement is widely perceived to be one of the biggest hurdles faced by healthcare organizations (Carr, 2014). While setting up patient portals and electronic delivery options can be relatively simple, promoting consumer utilization and achieving widespread use of these portals use has posed challenges. The healthcare paradigm has shifted in recent decades from viewing the patient as incidental to the delivery of healthcare to a more patient-centric approach. The previous model of indirectly funding Medicare, Medicaid, or employers has been noted as one of the greatest flaws of the healthcare system by contributing to cost inflation (Carr, 2014). Recent trends have promoted patient-empowered care, but have generally transferred the burden of cost to the individual. The Affordable Care Act (ACA) stimulated this shift by creating insurance exchanges which allow insurers to directly reach consumers; however, these readily-available healthcare options now require higher monthly premium payments from shoppers. This new model proposes that as patients become increasingly financially liable, they become more invested in their healthcare trajectories.

Keywords: E-Computing, E technology, Healthcare, Insurance, Medicare, Medicaid

Manuscript first received: 2018-10-26, Manuscript accepted: 2018-11-19

Address for correspondence:
Danielle A. O'Leary, Duquesne University, Pittsburgh, PA, USA
E-mail: danielle.oleary@uhc.com

Joan M. Kiel, Department of Health Management Systems & Chairman of University HIPAA Compliance, Duquesne Univesrity, Pittsburgh, PA, USA
E-mail: kiel@duq.edu

CONSUMER HEALTHCARE TECHNOLOGY

The rapid expansion of new technologies entering the market together with the rise of patient-centric care are driving the demand for consumer-driven technologies in the healthcare industry. As noted in "The Explosion of Consumer Technology in Healthcare", the tech-driven approach to health and wellness has created a $500 billion a year industry in the U.S. which averages a 25% growth annually (Slone Partners, n.d.). The availability of increasingly powerful technology at decreasing costs has raised the capacity to gather and process data, communicate more effectively, and monitor the quality of care processes (Sands & Wald, 2014). While growing exponentially, one of the greatest obstacles to promoting healthcare technologies is protecting the integrity of patient data or personal health information (PHI).

One contributor to the ever-growing consumer healthcare technology industry is the prevalence of similar technology among prevailing and younger, burgeoning demographics. Enhanced access to health-related data is appealing to so-called "Millennials" who have surpassed the Baby Boomer generation in the workplace. These Millennials challenge the unwieldy, pricy, and antiquated healthcare system by requiring enhanced service delivery through on-demand data. Insurers and health systems are facing the challenge of meeting the needs of tech-driven Millennial consumers while remaining accessible to consumers who prefer the traditional delivery of services. For example, a digital-only approach will isolate those consumers who prefer physical means for communication (Davis, 2015). Full digital adoption will be realized only when these "traditional" patients become active participants in their care through web-based tools (Slone Partners, n.d.). A recent goal of most health systems is to enhance the consumer experience for all, not just the tech-savvy.

ELECTRONIC DELIVERY

Advancements in consumer-driven healthcare technologies range from user-friendly online portals to artificial intelligence devices capable of analyzing large volumes of data and providing individualized recommendations and guidance (Cornille, 2016.); although vastly different, both relate to ways in which health data is delivered to patients. No matter the technology discussed, the perception of a successful delivery varies among demographics. Evidence has shown that effective communication between consumers and insurers leads to increased satisfaction and improved health outcomes. For health insurers, the most fundamental forms of communication are member-facing materials including brochures, welcome packets, and health statements. Although proven to be operationally beneficial, healthcare companies are hesitant to move from the print and fulfillment of customer-facing documents to Electronic Delivery (eDelivery) options.

Electronic Delivery enables healthcare systems to deliver documents in an electronic format rather than have them printed and delivered through the U.S. Postal Service. One form of eDelivery involves transmitting communications such as appointment reminders and health statements to an e-mail address provided by the consumer. These e-mail notifications are often linked to a secure member portal where authentication is required for access. Member portals are web-based applications that combine electronic health record (EHR) systems with a user-friendly interface. These portals assist members in carrying out self-management activities, thereby making the use of the system more effective not only from the standpoint of the consumer but also from the financial perspective of the organization. (Tavares, Oliveira, 2016).

Although research has shown that the adoption of eDelivery options will improve outcomes for enterprises, individuals, and the healthcare system as a whole, little consideration has been paid to the organizational structures and processes that drive the adoption of eDelivery. This paper will provide a conceptual framework for understanding eDelivery adoption by insurers. Specifically, this paper will highlight the key barriers faced by health organizations during different phases of the adoption process, financially and organizationally, along with the challenges faced by consumers, including accessibility and demographic make-up. This discussion will assess the potential of eDelivery and the currently demonstrated organizational reality and suggest how health insurers can close the gap.

HIPAA, HITECH, AND MEANINGFUL USE

On August 21, 1996, the U.S. Department of Health and Human Services (HHS) issued the Security Rule to implement the requirement of the *Health Insurance Portability and Accountability Act* (HIPAA) in an effort to establish a set of national standards for the protection of personal health information (PHI). HIPAA regulations require privacy standards to ensure the security of PHI while allowing the flow of health information needed to provide and promote high quality health care while also protecting the public's health and well-being (Office for Civil Rights [OCR], 2013). Through HIPAA, all of an individual's identifiable health information held or transmitted by a covered entity or business associate must be protected; in this context, a "covered entity" or "business associate" refers to insurers, clearinghouses, and providers.

Through Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), the Health Information Technology for Economic and Clinical Health (HITECH) act was established in an effort to stimulate the adoption of electronic health records (EHR) and other supporting technologies (Rouse, 2018). HITECH has yielded unprecedented levels of investment in health information technology (HIT) by incentivizing healthcare organizations to adopt the more modern technology available, eventually penalizing systems for continual reliance on conventional, paper-based processes (Avgar, Litwin, & Pronovost, 2012). As reinforcement to HIPAA regulations, HITECH was enacted not only to stimulate health information technology advancements in the United States but also to establish improved privacy and security provisions as they relate to PHI. This symbiotic relationship is demonstrated thusly: HIPAA established rules to hold business associates accountable for data breach liability where HITECH established data breach notification rules. In the context of HITECH, breach notification includes alerting impacted individuals, the Secretary of the Department of Health and Human Services, and in some instances, media outlets.

In conjunction with promoting the secure adoption of health information technology, the HITECH Act developed the concept of "meaningful use". Meaningful use in relation to HIT, defines minimum government standards for using PHI and for exchanging data between healthcare entities and their consumers (Rouse, 2010). Through meaningful use, health systems are provided with incentives to adopt HIT infrastructures while utilizing them in ways that improve quality, safety, and efficiency (Blumenthal & Tavenner, 2010). Implementing meaningful use was designed to unfold over three stages beginning in 2011, including: (1) Promotion of basic EHR adoption and data gathering; (2) emphasizing care coordination and exchange of patient information; and (3) improving overall healthcare outcomes (Practice Fusion, n.d.). While having good intentions, the goals of meaningful use have proven to be more challenging to achieve than originally anticipated. Striking a balance between financial resources, technical expertise, and infrastructure has posed obstacles for health systems. For health insurers who process large amounts of confidential health information in the form

of health statements and other communications, the increasing number of covered individuals poses challenges when adhering to the ethical obligations outlined in the HIPAA and HITECH.

STANDARDS FOR PROTECTING PERSONAL HEALTH INFORMATION

Using new health information technologies, individuals can better serve as intermediaries of the exchange of their information, promoting person-centered health (Patel, Barker, & Siminerio, 2015). The second stage of meaningful use essentially promotes the utilization of patient portals and electronic communications (including electronic statements) to engage and empower consumers. Prior to the launch of Stage Two in 2014, an assessment of electronic delivery receipt was conducted by the Healthcare Consumer Survey. Out of the 500 U.S. citizens surveyed, 60% of those receiving paper statements expressed interest in receiving electronic communications, citing instant access and convenience as the most appealing aspects (Hodges, 2014). Those who remain skeptical of eDelivery cited concerns regarding security and reliability.

In speaking with the Director of Transactional Communications for a Fortune 500 health insurer, it was noted that, "PHI is more valuable than financial records; insurers must abide by the highest levels of security with internal databases" (personal communication, June 11, 2018). If compromised, data contained in PHI could be used to steal identities, obtain health services, submit false claims, order pharmaceuticals, and perform other illegal acts. Further, cybercriminal activity has the potential to persist for months until detected, exacerbating its potential impact (Arnold, n.d.). The HIPAA Security Rule requires all covered entities to enact a security plan which contains three components: (1) administrative safeguards; (2) physical safeguards; and (3) technical safeguards. The breadth of the security plan is contingent upon specific factors such as the size of the organization.

HIPAA requires administrative safeguards such the development of a formal security management process that aids in identifying risks, designates a security official, provides adequate employee training, and outlines a plan for periodic assessments of security policies and procedures (45CFR164.308)[1]. For health insurers, these safeguards are demonstrated through annual HIPAA Compliance attestations, anonymous Compliance hotlines, and designated Compliance officers. Another important aspect of developing an administrative safeguard involves defining levels of access for all staff (Hicks, 2016). Assigned security responsibility is role based; thus if one needs access to PHI to complete their job functions, it will be granted (45CFR164.308(a)(3)(i)[2]. Physical safeguards include limiting unauthorized access to facilities, work stations, and devices. Providing secure locations for filed PHI, employee badges, along with the transfer, destruction, and disposal of PHI are all fundamental examples of physical safeguards. One example shared by a Subject Matter Expert (SME) includes the inability of employees to insert personal USB drives into device ports. This bars the potential transfer of data to and from the device, thus protecting the integrity of the data stored on the machine (SME, personal interview, June 11, 2018). Although administrative and physical safeguards are critical to an organization's security plan, when it comes to eDelivery, establishing effective and efficient technical safeguards is paramount to the security of PHI.

---

[1] (45CFR164.308). 45CFR Parts 160, 162, and 164. Department of Health and Human Services. Security Standards: Final Rule. February 20, 2003.

[2] (45CFR164.308(a)(3)(i). 45CFR Parts 160, 162, and 164. Department of Health and Human Services. Security Standards: Final Rule. February 20, 2003.

With regard to technical safeguards, the Security Rule is based on the fundamental concepts of flexibility, scalability, and technology neutral. There are no specific requirements for the types of technology to be enacted; the onus falls on the covered entity to determine the appropriate security measures and specific technologies appropriate for their own organization given its unique characteristics (The U.S. Department of Health and Human Services [HHS], 2007). Although each individual organization has liberties in choosing its technological infrastructures to employ, there are several general minimum requirements outlined by the Security Rule that must be met. While there are myriad solutions to choose from, several examples of technical safeguards were noted by SMEs through personal interviews.

The first standard outline by the Security Rule relates to Access Control. Access is defined as the ability or the means necessary to read, write, modify, communicate data, or use any system resource. Authorized users should be given access to the minimum necessary information to perform job functions. Practically, authorizing all users to access potentially millions of individuals' PHI would pose an enormous risk of jeopardizing the security of that data, so processes and standards must be developed for limiting the ability to read and modify data to only those necessary. Through the Security Rule, there are two implementation specifications that organizations must adhere to: (1) unique user identification and (2) emergency access procedure. (45CFR164.312(2)(i) & (ii))[3]. Unique user identifiers refer to an alpha, numeric, or alpha/numeric user name that can be used to trace activity. These identifiers are typically assigned in uniformity according to the standards of the organization. Randomly generated identifiers consisting of a combination of alpha and numeric characters are more secure; however, such identifiers can be difficult for the user to remember. Some organizations employ the use of Single Sign-On (SSO) Authentication whereby the user is securely logged into all of the appropriate systems needed for day-to-day operations, eliminating the need for users to remember multiple passcodes. Emergency access procedures are established and implemented in the event that PHI must be electronically retrieved in the event of an emergency. Of course, these procedures must be established and communicated prior to the disaster in order to be effective, so health organizations have been wise to plan ahead.

Audit Controls are the second standard established through the Security Rule. Audit functions track and examine the activity within a system where PHI is stored or accessible. The unique member identifiers required under the Access Control standard can be linked to the user's footprint within a system, and audits put can recreate those footprints into a path to ensure the employers' standards are maintained. The misuse or inaccurate access of PHI can and should be traced, with any compromise in integrity reported to the proper compliance officer. Although Audit Controls are required, the degree of granularity kept in the data logs can vary by what the organization deems useful (Arnold, n.d.).

Data Integrity, the third standard under the Security Rule, requires an organization to ensure that data or information has not been accessed, altered or destroyed in an unauthorized manner (HHS, 2007). Compromised integrity can be the result of user error or device failure and may lead to significant patient privacy issues and data breaches, and can erode confidence in an organization. Data authentication processes can ensure that PHI has not been subject to alteration or misuse. Person or Entity Authentication are the fourth standard of the Security Rule, referring to the procedures that verify the identity of the individual or entity seeking access to PHI. Identity must be verified through

[3] (45CFR164.312(2)(i) & (ii)). 45CFR Parts 160, 162, and 164. Department of Health and Human Services. Security Standards: Final Rule. February 20, 2003.

a unique passcode or pin established by the user. For added security, some devices are equipped with biometrics that require fingerprints, iris patterns, or voice controls.

Transmission Security is the final safeguard outlined by the Security Rule, requiring the secure communication of information across internal and external networks. One appropriate means of protecting the integrity of the transferred data includes encryption, whereby data is stored and transferred in a format that only another secure user with the specific encryption key (or using the same secure program) can gain access. The protocols for Transmission Security are oftentimes more rigid for third party vendors in order to maintain strict compliance with data protection standards. Firewalls protect an organization's internal data sources and vendors must engage in rigorous and costly certifications to gain what's known as "Tier 1" access. Tier 1 access refers to a limited right of entry whereby vendors may only access information relevant to their services (SME, personal interview, July 9, 2018).

Despite organizational efforts to protect PHI, approximately 1.13 million patient records were compromised in data breaches in the first quarter of 2018. 77.1% of these incidences were the result of privacy violations by business associates, signifying that the Access Control regulations for some organizations are falling short (Donovan, 2018). Entities are required to notify the Department of Health and Human Services and the media immediately about potential breaches if it affects more than five hundred customers. The five largest health insurance payers in the United States serve between fifteen million to seventy million subscribers, rendering a data breach of five hundred or more victims very likely in the event of an intentional breach. According to a 2017 article, seventy percent of Americans distrust health technology, specifically citing publicized PHI data breaches (Shaw, 2017).

ORGANIZATIONAL ADOPTION OF ELECTRONIC DELIVERY METHODS

Health information technology adoption, specifically the promotion of eDelivery methods, is a complex and multi-staged process that requires more than installing hardware, software, and peripherals. Research suggests that implementations of HIT advancements are driven by organizational features as opposed to technological. In fact, it is organizational stakeholders at varying levels determining how to respond to the demands of the external environment through workplace innovations (Avgar, Litwin, & Pronovost, 2012). Aside from customer satisfaction, the main factor that drives strategic IT change is reducing administrative costs.

For insurers, investing the capital into eDelivery developing, implementing, and maintaining eDelivery technologies is more cost-effective than traditional print and fulfillment. Large insurance companies spend over $400 million in print and postage per year (SME, personal interview, June 11, 2018). This figure does not factor in the costs associated with third party vendor software to track and trace individual mail items. The recent implementation of the Affordable Care Act (ACA) introduced what is commonly known in the industry as "1557 taglines". Under Section 1557 of the ACA, the law prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in certain health programs or activities (OCR, 2018). Through this provision, insurers are required to print non-discrimination notices along with translation support in preferred languages on specified member-facing materials. The regulation to add these disclaimers has increased print costs by over $50 million. Needless to say, full adoption of e-delivery would greatly diminish these overhead costs.

Developing and promoting eDelivery technologies also has the potential to improve the end-customer experience, improve message simplicity, decrease call center inquiries, and influence consumer behavior with advanced messaging (Buckley, N.D.). Realizing these benefits requires more than just switching from paper to e-mail delivery. Interactive and informative patient portals enhance the customer experience promoting frequent active usage of the portal and eDelivery methods. When making the decision to invest in eDelivery, insurers must take into account all of the impacted applications and associated processes to ensure the final product is streamlined for optimal customer engagement. eDelivery technologies have the potential to provide meaningful use. Approaches such as advanced messaging can promote health and wellness incentive programs which increase beneficiary involvement and decrease overall cost (SME, personal interview, June 11, 2018). Despite the appeal, eDelivery attainment rates remain low for healthcare organizations due to a number of internal and external barriers.

INTERNAL BARRIERS TO ELECTRONIC DELIVERY PROMOTION

Health organizations large and small are making the transition from "legacy systems" to newer HIT platforms such as Epic. In HIT, a legacy system refers to older clinical technology that may no longer support the needs of the organization. These clinical technologies may refer to a claims adjudication system (CAE) which may be monolithic and dated that do not effectively support specialty lines of business or growing healthcare complexity (Hart, 2011). Legacy systems may also refer to obsolete mainframe operating systems or hardware that has not yet been replaced with Linux, Unix, or Windows, for example. Lastly, they may refer to outdated programming languages. New industry standards have given rise to open source languages such as Java (Newman, 2016).

Well-established organizations may consist of many legacy technologies across varying product lines. In most instances, these systems are not compatible with one another making integration difficult. Another potential added layer of complexity arises when the system data is not "normalized". Normalization is the process of standardizing and organizing data within a database which includes establishing relationships between datasets according to rules designed to both protect data and eliminate redundancy (Wambler, n.d.). Non-normalized data requires the user to manually manipulate data to be used for analysis. Given the potential variety of business segments within a large healthcare organization, it is difficult to establish an enterprise wide strategy for promoting eDelivery. The various segments often silo themselves according to the limitations of their legacy technologies and develop siloed approaches further contributing to system disconnects. eDelivery adoption and adherence remains low not only due to organizational and technological limitations but to external consumer attributes as well.

EXTERNAL BARRIERS TO ELECTRONIC DELIVERY PROMOTION

The introduction of the Affordable Care Act expanded the membership spectrum for many Health Maintenance Organizations (HMOs). These HMOs have broadened their membership horizon by offering Medicaid and Medicare Management Plans along with providing more options for individuals and employers through the healthcare exchanges. Medicare, Medicaid, Employer-sponsored, and Individually-sponsored plans are the four predominant beneficiaries served by insurers. Promoting the adoption of eDelivery among these business segments poses unique challenges.

Medicare beneficiaries are often 65 and older and are oftentimes referred to as "traditional" patients who prefer direct communication as opposed to indirect. These older adults are one population in which the vast majority have one or more chronic health condition that could stand to benefit from resources provided by the internet (Zulman, Kirch, Zheng, & An, 2011). According to a 2018 statistic, 66% of adults 65 and older are internet users (Statista, n.d.). Compared to 98% of the 18 to 29 year old age group who utilize the web, this figure suggests that the 65 and older crowd is lagging in internet adoption. Not only do disparities exist age-group to age-group but are apparent within the groups themselves. When it comes to engagement in eDelivery through their member portals, a recent study revealed that 65% of beneficiaries reported being connected to their online accounts but only 20% use it regularly. Print fulfillments and telephone calls remained as the preferred method of communication for health plan interactions (HealthMine, 2017).

Research has been conducted on the internet usage disparities among older adults with respect to overall health and socioeconomic status. Approximately 30% of adults with annual household incomes below $30,000 do not own a smart phone. In addition, almost 50%, do not have broadband services or a computer at home. But for households with an annual household income of $100,000 or more, nearly 100% of people have a smart phone, broadband services and a computer (Anderson, 2017). In regards to health status, those with chronic illnesses such as Alzheimer's reported lower internet usage rates; however, adults diagnosed with *manageable* chronic illnesses such as diabetes displayed higher usage rages. Research suggests that the strongest determinants of usage are educational attainment and income level. Compared to college graduates, high school graduates were 80% less likely to access the internet. One determinant older adults share is overall trust with electronic materials. This distrust is may be due to the difficulty with assessing online credibility or believability. This population of individuals might find the process of assessing the credibility of online materials as overwhelming leading to a general distrust of HIT (Choi & DiNitto, 2013).

Medicaid beneficiaries tend to have limited internet access due to lower economic status. In speaking with a field expert (personal interview, July 9, 2018), it was reported that Medicaid recipients do not have access to computers while 74% have smart phones. Given that health insurers are overall "late adopters" when it comes to HIT, the development of mobile insurance applications is in its infancy. Similarly to Medicare beneficiaries, it has been suggested that Medicaid recipients could benefit from online engagement with their health plans. In 2017, it was reported that Medicaid costs accounted for 17% of the U.S. health care expenditure with 72.2 million recipients (Statista, n.d.). This upward enrollment trend suggests that insurers will continue to expend exorbitant print and fulfillment costs and financial penalties as a result of poor health outcomes if eDelivery options remain unexplored.

Employer-sponsored and individually-sponsored consumers are reportedly the highest adopters as they tend to be younger, employed, and of higher income. Due to the fact that these groups oftentimes have a choice between health plans, they are typically more educated about their options as a product beneficiary. Some insurers offer eDelivery only plans to interested consumers. Enrolled parties may receive financial incentives such as discounted premiums or Health Savings Account (HSA) contributions.

RECOMMENDATIONS FOR PROMOTING ADOPTION

In order to implement successful eDelivery strategies, organizations must understand the unique internal and external challenges that they may face in promoting adoption. By understanding these barriers, organizations can create proactive business approaches and tailor electronic services to the preferences of the customer. Streamlining the organizational goals and internal systems may lead to more reliable and accurate systems. Direct and indirect consumer engagement efforts, such as phone campaigns or focus groups, may also contribute to successful adoption by changing perceptions on trust, security, and accessibility. In conclusion, the ability to promote health information technologies such as eDelivery options and patient portals is highly contingent on the organizations ability to define, invest, development, and utilize these new technologies while adhering to industry standards and government regulations.

REFERENCES

Anderson, M. (2017). Digital Divide Persists Even as Lower-income Americans Make Gains in Arnold, N. (N.D.). PHI Security and Auditing: Reducing Risk and Ensuring Compliance with a Data Warehouse. [Web Blog]. Retrieved June 28, 2018, from: https://www.healthcatalyst.com/PHI-security-auditing-reducing-risk-ensuring-compliance

Avgar, A. C., Litwin, A. S., & Pronovost, P. J. (2012). Drivers and Barriers in Health IT Adoption: A Proposed Framework. Applied Clinical Informatics, 3(4), 488–500. Retrieved June 13, 2018, from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3631941/

Blumenthal, D., Tavenner, M. (2010, Aug. 5). The "Meaningful Use" Regulation for Electronic Health Records. The New England Journal of Medicine, 363: 501-504. Retrieved June 28, 2018, from: https://www.nejm.org/doi/10.1056/NEJMp1006114

Buckley, L. (N.D.). No Title. Retrieved July 20, 2018, from: https://www.dataoceans.com/2014/06/06/electronic-adoption-solutions-for-the-healthcare-industry/

Carr, D.F. (2014, Jan. 31). What Consumer-Driven Healthcare Really Means [Commentary]. Retrieved June 13, 2018, from: https://www.informationweek.com/healthcare/patient-tools/what-consumer-driven-healthcare-really-means/d/d-id/1113649

Choi, N. G., & DiNitto, D. M. (2013). Internet Use Among Older Adults: Association With Health Needs, Psychological Capital, and Social Capital. Journal of Medical Internet Research, 15(5), e97. Retrieved July 27, 2018, from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3668603/

Cornille, S. (2016, Aug. 23). The Future is Nigh: Nine ways consumer driven technology will fundamentally redefine healthcare [Web Blog]. Retrieved June 13, 2018, from: https://orionhealth.com/us/knowledge-hub/blogs/the-future-is-nigh-9-ways-consumer-driven-technology-will-fundamentally-redefine-healthcare

Davis, J. (2015, Nov. 20). Healthcare in 2016: consumer-driven [Web Blog]. Retrieved June 13, 2018, from: https://www.healthcareitnews.com/news/2016-health-technology-prediction-consumer-driven-healthcare

Donovan, F. (2018, May 7). 1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018. [Web Blog]. Retrieved July 6, 2018, from: https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018

Hart, E. (2011, Jul. 1). How agile is your claims adjudication system? [Web Blog]. Retrieved July 20, 2018, from: https://www.healthmgttech.com/how-agile-is-your-claims-adjudication-system.php

HealthMine. (2017, Jun. 12). Medicare Recipients 65+ Use Their Health Plan's Portal Regularly, HealthMine Survey. [Survey]. Retrieved July 27, 2018, from: https://www.prnewswire.com/news-releases/just-20-of-medicare-recipients-65-use-their-health-plans-portal-regularly-healthmine-survey-300472293.html

Hicks, J. (2016, Nov. 22). Three Safeguards to Reduce Risks to PHI. [Web Blog]. Retrieved June 28, 2018, from: https://www.verywellhealth.com/safeguards-to-reduce-risks-to-phi-2317519

Hodges, C. (2014, May). Electronic Statements Engage Patients and Increase Prompt Payment [Web Blog]. Retrieved June 28, 2018, from: http://www.hfma.org/Content.aspx?id=22683

Newman, D. (2016, Jan. 7). Legacy System. [Quick Read]. Retrieved July 27, 2018, from: https://healthcareitskills.com/legacy-system/

Office for Civil Rights (HHS.gov). (2013, Jul. 26). Summary of the HIPAA Privacy Rule. Retrieved June 13, 2018, from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#

Office for Civil Rights. (2018, Apr. 15). Section 1557 of the Patient Protection and Affordable Care Act. Retrieved July 6, 2018, from: https://www.hhs.gov/civil-rights/for-individuals/section-1557/index.html

Patel V., Barker W., & Siminerio E. (2015, Oct.). Trends in Consumer Access and Use of Electronic Health Information. ONC Data Brief, no.30. Office of the National Coordinator for Health Information Technology: Washington DC. Retrieved June 28, 2018, from: https://dashboard.healthit.gov/evaluations/data-briefs/trends-consumer-access-use-electronic-health-information.php

Practice Fusion. (N.D.). What is Meaningful Use? [Definition]. Retrieved June 28, 2018, from: https://www.practicefusion.com/what-is-meaningful-use/

Rouse, M. (2010, May). Meaningful Use [Definition]. Retrieved June 13, 2018, from: https://searchhealthit.techtarget.com/definition/meaningful-use

Rouse, M. (2018, Jan.). HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009. Retrieved June 13, 2018, from: https://searchhealthit.techtarget.com/definition/HITECH-Act

Sands, D. Z., & Wald, J. S. (2014). Transforming Health Care Delivery Through Consumer Engagement, Health Data Transparency, and Patient-Generated Health Information. Yearbook of Medical Informatics, 9(1), 170–176. Retrieved June 13, 2018, from: https://www.ncbi.nlm.nih.gov/pubmed/25123739

Shaw, G. (2017, Jan. 5). Patients don't trust health information technology. [Web Blog]. Retrieved July 6, 2018, from: https://www.fiercehealthcare.com/it/patients-don-t-trust-health-information-technology

Slone Partners (2016). The Explosion of Consumer Technology in Healthcare [Web Blog]. Retrieved June 13, 2018, from: http://www.slonepartners.com/explosion-consumer-technology-healthcare/

Statista. (N.D.). Medicaid - Statistics & Facts. [Statistics]. Retrieved July 27, 2018, from: https://www.statista.com/topics/1091/medicaid/

Statista. (N.D.). Share of adults in the United States who use the internet in 2018, by age group. [Statistics]. Retrieved July 27, 2018, from: https://www.statista.com/statistics/266587/percentage-of-internet-users-by-age-groups-in-the-us/

Tavares J., Oliveira T. (2016, Mar.). Electronic Health Record Patient Portal Adoption by Health Care Consumers: An Acceptance Model and Survey. Journal of Medical Internet Research, 18(3):e49. Retrieved June 13, 2018, from: http://www.jmir.org/2016/3/e49/

Tech Adoption. Fact Tank News in the Numbers, Pew Research Center. March 22, 2017. Retrieved October 10, 2018, from http://www.pewresearch.org/fact-tank/2017/03/22/digital-divide-persists-even-as-lower-income-

The U.S. Department of Health and Human Services. (2007, Mar.). Security Standards: Technical Safeguards. Retrieved July 6, 2018, from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=eS

Wambler, S. (N.D.). Introduction to Data Normalization: A Database "Best" Practice. [Web Blog]. Retrieved July 27, 2018, from: http://agiledata.org/essays/dataNormalization.html

Zulman, D. M., Kirch, M., Zheng, K., & An, L. C. (2011, Feb. 16). Trust in the Internet as a Health Resource Among Older Adults: Analysis of Data from a Nationally Representative Survey. Journal of Medical Internet Research, 13(1), e19. Retrieved July 27, 2018, from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3221340/americans-make-gains-in-tech-adoption/