Telerehabilitation Store and Forward Applications: A Review of Applications and Privacy Considerations in Physical and Occupational Therapy Practice

Christopher Peterson, PT, DPT, CERT. MDT[1] & Valerie Watzlaf, PhD, RHIA, FAHIMA[2]

[1]Hartford HealthCare Rehabilitation Network, Hartford, CT, USA

[2] Department of Health Information Management, School of Health and Rehabilitation Sciences, University of Pittsburgh, Pittsburgh, PA, USA

Abstract

An overview of store and forward applications commonly used in physical and occupational therapy practice is reviewed with respect to regulation, privacy, security, and clinical applications. A privacy and security checklist provides a clear reference of pertinent regulatory issues regarding these software applications. A case study format is used to highlight clinical applications of store and forward software features. Important considerations of successful implementation of store and forward applications are also identified and discussed.

Keywords: Asynchronous telehealth, business associate, business associate agreement, covered entity, HIPAA HITECH, occupational therapy, physical therapy, privacy, Protected Health Information (PHI), security, tele-PT, telerehabilitation

Telerehabilitation (TR) store and forward applications are being used for physical therapy (PT) and occupational therapy (OT) services. The tele-therapy apps enable a physical therapist, occupational therapist, or other provider to offer PT and OT services to clients who may not be able to access their services in a provider's clinical setting. These apps can also be utilized in conjunction with traditional care to extend exercise instruction more seamlessly into the home by use of digital images, video, text messaging, etc. This can be very beneficial for both the client and therapist. However, before physical or occupational therapists decide to use tele-therapy apps they should first determine whether the health information that is transferred, stored and shared within the company that developed them is private and secure and will meet the HIPAA requirements.

When deciding on what type of store and forward app to purchase it will be important to survey the clinical needs that such a program will fulfill. Targeting the specific aims of therapeutic programs, assessing staff training needs, and identifying a plan of integration for PT/OT apps within any existing IT frameworks will be important. Consideration of these elements will result in the most targeted integration of store and forward apps into PT or OT practice.

Health information is highly regulated. Information obtained via tele-therapy apps is no exception. The most familiar regulation impacting healthcare facilities and providers is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a federal law that provides privacy and security rules and regulations to protect personal health information. Before HIPAA, however, there were many federal and state laws that governed the use and disclosure of health information. These include:

1. The Freedom of Information Act of 1974 (FOIA)
2. The Privacy Act of 1974
3. The Drug Abuse Prevention, Treatment and Rehabilitation Act of 1972
4. The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970

5. The Medicare Conditions of Participation
6. The American Recovery and Reinvestment Act (ARRA) and Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
7. Varied state laws on privacy and security of health information.

Of these laws, the HIPAA and HITECH Acts have provided the most specific and stringent regulations for the protection of the privacy and security of health information. However, some state regulations may be more stringent and, if so, should be followed. Preemption applies to HIPAA and therefore, compliance with federal law when federal and state law conflict is required (Rinehart-Thompson, 2013).

The HIPAA Privacy Rule is an administrative law created by the Department of Health and Human Services (DHHS). It was developed after the HIPAA statute was passed by the US Congress and went into effect in 2003. The HIPAA Privacy Rule only applies to healthcare providers that conduct electronic billing transactions -- but is effective for both paper and electronic health information.

The HIPAA Security Rule went into effect in 2005 and regulates only electronic health information.

The HITECH Act includes changes to the HIPAA Privacy and Security rules that focus mainly on health information technology and strengthens standards for the privacy and security of health information. It went into effect in 2010 but some parts of the act have different compliance deadlines (Rinehart-Thompson, 2013).

PROTECTED HEALTH INFORMATION

Health Information must meet a three part test to be considered protected health information (PHI).

First, it must identify the person outright by using his/her name or image or provide enough information so that the person could be identified using one or more of the 18 HIPAA identifiers (i.e., names, geographic subdivision, dates, telephone numbers, fax numbers, email addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate and license numbers, vehicle identifiers, device identifiers, URLs, IP address numbers, biometric identifiers, photos, and any other unique identifying number, characteristic or code). Second, it must also relate to an individual's past, present, or future physical or behavioral health condition or provision of healthcare or payment for the provision of healthcare. Third, it must also be kept or transmitted by the covered entity or its business associate in any form or medium, including electronic, paper or oral (Rinehart-Thompson, 2013; HHS, 2007).

If PHI exists in any form (i.e., paper, electronic, video, verbal conversations), the HIPAA Privacy Rule applies. However, the HIPAA Security Rule only applies to electronic PHI. It is recommended that the covered entity and business associate strive to protect the privacy and security of all PHI at all times and not separate out what applies to the privacy rule and what applies to the security rule.

COVERED ENTITY

A "covered entity" (CE) is the organization that must comply with all HIPAA and HITECH regulations when dealing with health information. Covered entities include:

1. Healthcare Providers: Refers to all healthcare providers who transmit data electronically (e.g., physical therapists, occupational therapists, speech-language pathologists, physicians, psychologists, dentists, chiropractors). This category applies to healthcare sites such as clinics, hospitals, nursing homes, pharmacies, and all other healthcare providers that transmit data electronically.
2. Health Plans: Refers to an individual or group plan that provides or pays the costs of medical care, such as health insurance companies, HMOs, company health plans, and government programs that pay for health care (e.g., Medicare, Medicaid, and the military and veterans' health care programs).
3. Healthcare Clearinghouses: Refers to entities that process nonstandard health information they receive from another entity into a standard format (i.e., standard electronic format or data content), or vice versa (HHS, 2007; HHS, n.d.).

BUSINESS ASSOCIATE

A business associate (BA) according to HIPAA, includes any entity that works on behalf of the CE and that creates, receives, maintains, or transmits individually identifiable health information. Examples may include the following:

1. A person that offers a personal health record to one or more individuals on behalf of a CE;
2. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the BA; or
3. Organizations that perform services for the CE that involve health information, such as claims processing,

data analysis, utilization review, quality assurance, client safety activities and so forth (HHS, 2007).

The HIPAA and HITECH Rules apply to covered entities and business associates. If an entity does not meet the definition of a CE or BA, it does not have to comply with the HIPAA Rules.

BUSINESS ASSOCIATE AGREEMENT

Individuals, organizations, and agencies that meet the definition of a CE under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information. If a CE works with a BA to help it carry out its health care activities and functions, the CE must have a written Business Associate Agreement (BAA) with the BA. The BAA must specifically state what the BA has agreed to do and requires the BA to comply with the HIPAA and HITECH rules to protect the privacy and security of PHI. In addition to these contractual obligations, BAs are directly liable for compliance with certain provisions of the HIPAA and HITECH Rules and can face the same fines and penalties as the CE for breach of PHI (HHS, n.d.).

Even though a telerehabilitation store and forward company is not listed specifically in the above definition of a BA, is it, when used for telerehabilitation, considered a BA of a CE if the CE is the healthcare system, therapy clinic or provider? If so, the CE would need to enter into a BAA with the telerehabilitation company and must have systems in place to meet the HIPAA and HITECH requirements. Telerehabilitation store and forward companies and the entities that use them for telerehabilitation purposes will need to comply with the HIPAA and HITECH regulations since they would be considered a BA.

Once the CE works with a person or organization that the CE determines is a BA, it is the CE's responsibility to initiate a BAA with that BA. Elements of a BAA can be specific and lengthy. A sample BAA can be found at the Office of Civil Rights under Health Information Privacy (HHS, 2013) and is available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

DATA USE AGREEMENT

A data use agreement (DUA) is required if the PHI includes direct identifiers. The scope of a DUA includes the data that is collected, stored, transferred, and methods of destruction of the data once the data conversion is completed by the BA for the work that is being done between the BA and the CE. It can also outline how that data can be used by the BA. For example, while a CE may not want the BA to use the data that they are collecting for research purposes, the CE may deem it acceptable for the BA to use the data to provide feedback to their clients. The DUA provides specificity in how data can be used between the CE and BA.

The terms of the DUA are housed within a separate, dedicated document, but in some cases, can be consolidated within the BAA (i.e., as one document that meets HIPAA requirements). If, however, the CE provides the BA with PHI that includes direct identifiers, a DUA is required in addition to the BAA (HHS, 2006).

UNRESOLVED DATA ISSUES

Personal health and fitness data, data collected from videos of therapy exercises performed by clients and recorded by their healthcare providers, and data collected from fitness bracelets and other exercise applications, all have the potential to be sold to third parties. The FTC is concerned, but has not required companies to provide an opt-out option for their users. The FDA released guidelines on mobile medical applications, but this only applies to those applications that are used for medical diagnosis and treatment (Schumer, 2014).

A recent study found that less than a third of popular health apps have privacy policies and those that do are not clear and understandable to the user and are not focused on the use of the app itself (Sunyaev et al., 2014). This was also found in a study by Cohn and Watzlaf (2012) in which Voice over Internet Protocol (VoIP) websites privacy policies were examined and found to be difficult to understand when measured by readability scales.

NEED FOR A PRIVACY AND SECURITY CHECKLIST

Could telerehabilitation store and forward applications and the companies that develop them face a similar dilemma? Do they provide appropriate privacy and security policies to their users and are they HIPAA compliant? What is done with the video and/or data content that is stored and forwarded to clients and healthcare providers? How is the privacy and security of this data maintained?

Every healthcare provider that is considering using this service should consider the benefits and the risks of using it. In order to help healthcare providers make their decision, a privacy and security checklist is provided in Table 1. It is recommended that providers investigate each of the telerehabilitation companies that they are considering using and employ the checklist to determine if the benefits

outweigh the risks. Once this is complete, providers should consider the practical applications of implementing the technology into their practice.

Table 1. Privacy and Security Compliance Checklist for Telerehabilitation Store and Forward Applications

PRIVACY	Yes	No	Not Included in Policy	Notes
I. Accessibility of Personal Information				
Will employees of the telerehabilitation company have access to client identifiable data and/or video?				
Will data and/or video generated during therapy sessions between the therapist and client be accessible to other users/consumers outside of the telerehabilitation company?				
Will data and/or video generated during therapy sessions between the therapist and client be sold to other marketers, insurance companies, or other interested parties?				
Will data and/or video stored at the telerehabilitation company be shared to protect the company's legal requirements, interests, enforce policies or to protect anyone's rights, property or safety?				
Will data and/or video from the telerehabilitation company be shared with any other business associates?				
II. Amendment of Personal Information				
Will the telerehabilitation company provide the user 30-60 days to comply with a new privacy policy, if it has changed?				
Will the user be able to change or add or delete any personal information within a reasonable period of time?				
III. Retention of Personal Information				
Are video and/or data generated between the therapist and client retained by the telerehabilitation company?				
How long will the video and/or data stored by the telerehabilitation company be retained?				
Will other PHI be retained?				
What other types of PHI will be retained? For how long?				
Do users get the option of archiving their records offline on storage network devices?				
IV. Requests for Information				
Will data and/or video content be made available to other entities when requested?				
Will client authorization be required before any personal information, data and/or video content is shared with other requestors?				
Will a qualified individual in health information management with privacy, confidentiality and HIPAA compliance experience analyze all requests for PHI?				
Will a subpoena or court order be requested from law enforcement and government officials requesting personal information, data and/or video content of the client?				
Will a complete and accurate accounting of disclosures be made to the client?				
Are clients able to request a restriction of uses and disclosures?				
V. Sharing of Personal Information with other Countries/Websites				
Will the telerehabilitation company transfer PHI outside the country of origin to a third				

party?				
Will the client have the right to consent to any transfer of PHI outside of his/her country?				
If the client authorizes and consents to the transfer of PHI outside of his/her country, will a list of countries where this PHI will be transferred be provided to the client?				
Will the telerehabilitation company's software contain links to other websites that may have a different privacy and security policy than their policy?				
VI. Business Associate (BAA) and Data Use (DUA) Agreements				
Does the telerehabilitation company maintain a business associate agreement with the covered entity (healthcare provider)?				
Will the telerehabilitation company obtain business associate agreements with each of the other websites in which personal information may travel?				
Will a data use agreement that provides more specific uses of data collected between the CE and BA be added to the BAA?				
SECURITY				
VII. Encryption				
Is any transfer of video and data content encrypted with strong encryption algorithms that are private and secure during transmissions?				
Does the encryption protect the transfer of data and/or video content to all types of media devices including smart phones, tablets, laptops, personal computers, etc.?				
Are encryption details explained in the privacy and security policy of the telerehabilitation company?				
Can a third party decode a video and/or data content by accessing encryption keys?				
VIII. User Procedures				
Are users made aware of the importance of having anti-virus and anti-spyware protection on their computer or mobile device to prevent misuse of their personal information when transferred from the telerehabilitation company to them?				
Are clients informed of the potential security risks when video and data content are transferred between their healthcare provider and the telerehabilitation company and between the client and the telerehabilitation company?				
Are clients informed of the security issues in their informed consent?				
Are users encouraged to use remote wiping, firewalls, security software and keep it up to date, research mobile applications before downloading, maintain physical control of the mobile device and do not use public Wi-Fi when transferring PHI?				
IX. Audit System Activity				
Are audit trails used to track who had access to personal identifiable video and/or data content?				
Are access controls put in place so that only individuals with appropriate roles in the telerehabilitation company are accessing video and/or data content with PHI?				
Is a unique user identification (e.g., username, password, additional authentication), provided to every employee that has access to PHI?				

Are all employees of the telerehabilitation company provided with privacy and security awareness training?				
Has a security evaluation of the telerehabilitation store and forward company been performed by an independent group?				
Does the security evaluation include authentication, password management, data management and verification that the telerehabilitation store and forward company implements all proper privacy and security measures?				
X. Overall Assessment of Privacy and Security				
Does the telerehabilitation company meet HIPAA requirements? (HIPAA Audit Protocol can be used for evaluation) http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html				

PRACTICAL CASE STUDY: OUTPATIENT PHYSICAL THERAPY

Mary arrives to an outpatient physical therapy clinic for post-operative rehab following right knee anterior cruciate ligament (ACL) reconstruction. In adherence to a partial weight-bearing precaution as per her referring physician, she is unable to walk without the use of an assistive device. Functionally, this limits her performance of ADLs and her ability to perform normally at work as a cashier. Her insurance covers physical therapy with a $50.00 co-pay per visit. Two proposed models for the provision of physical therapy services are outlined. Benefits of store and forward features are discussed in Table 2.

1. Physical therapy assessment and treatment in a traditional clinical setting featuring one-on-one in-person care 2-3 sessions per week for 8-12 weeks with a telerehabilitation store and forward company used for provision of a home exercise program (HEP) and client education materials.
2. Physical therapy assessment and treatment in a traditional clinical setting featuring one on one in person care 2-3 sessions per week for 8-12 weeks with a cloud based software solution that includes mobile device access and email capability used for dissemination of HEP materials.

Table 2. Benefits of Asynchronous (Store and Forward) Features

Feature	**Potential Application/Benefit**
Sketch Images	Clarify body mechanics, pre-set and post-set positions of prescribed exercises and targeted functional activities.
Photographic Images	Clarify body mechanics, pre-set and post-set positions of prescribed exercises and targeted functional activities.
Video Content	Clarify dynamic positions related to prescribed exercises and functional activities.
Flow Sheet	Allow for a means to enter data and track program compliance and progression. (Future programs will try to leverage biometric data collected from mobile devices to automatically populate these flow sheets.)
Client Education Modules	Provide clients with clear advice that they can use now and to help address future episodes. Modules will likely incorporate text, still picture, sketch pictures, and audio.
Mobile Technology access	The ability to access data will improve client compliance and increase client access to therapeutic recommendations made by the therapist.
Interactive Features	Incorporation of biometric data such as heart rate, respiratory rate, daily step count, etc. will help to identify a more complete picture of a client's daily function and fitness level.
Calendar Integration	Calendar integration can allow for reminders to be automatically integrated into cloud based calendars (such as Outlook and iCal) that will create alerts to help motivate clients and improve compliance with therapeutic recommendations.

Provider/client Interface (Email/SMS etc.)	This will allow for more immediate access to care. Troubleshooting problems with therapeutic programs between scheduled clinic visits could help keep clients tracking towards therapeutic goals and potentially eliminate additional clinic visits.
Social Media Component	Social media integration could potentially help to motivate clients; however this is a controversial topic. All state and federal regulatory statutes must be adhered to when considering any social media type features (refer to Table 1).
Integration with EMR	Seamless integration of cloud-based exercise software solutions with an electronic medical record (EMR) will allow providers to shift focus away from data collection and entry during clinical visits and concentrate on clinical analysis of data. This will become particularly true as biometric data is incorporated into these programs.
Integration with Biometric/gaming Interfaces	Increase ability to collect clinical data such as rate velocity of movement, accuracy of movement, functional capacity, aerobic capacity, etc.

CLOUD-BASED SOLUTIONS

Table 3 outlines the features of three cloud-based store and forward software solutions as compared to a commonly used non-cloud based solution that is widely used in physical and occupational therapy practice within the United States. These software and app solutions offer greater flexibility to both clients and therapists, allowing for more ease of access to HEP and education information.

Table 3. Comparison of Cloud-Based to Non-Cloud Based Solution Features

Feature	**Industry Standard**	**Cloud-based Solution A**	**Cloud-based Solution B**	**Cloud-based Solution C**
Sketch Images	Yes	No	No	No
Photographic Images	Yes	Yes	Yes	Yes
Video Content	No	Yes	Yes	Yes
Flow Sheet	Yes	Yes	Yes	Yes
Client Education Modules	Yes	Yes	Yes	Yes
Mobile Technology access	No	Yes	Yes	Yes
Interactive Features	No	Yes	Yes	Yes
Calendar Integration	No	No	Yes	Yes
Provider/client Interface (Email/SMS etc.)	No	Yes	Yes	Yes
Social Media Component	No	No	Yes	No
Integration with EMR	Yes	Yes	Yes	Yes
Integration with Biometric/gaming Interfaces	No	No	No	No

The features analyzed here are often included in cloud-based programs. The infrastructure of a robust store and forward program will allow for both dissemination of information in the form of individualized exercise protocols, and pre-established protocols as well as a series of interactive features that will allow clients and therapists to

track and even receive notifications about program compliance and program changes. Biometric data, such as the number of steps traveled in a day, heart rate, respiratory rate, etc. may also be provided through interfaces with measurement technologies that are becoming standard on mobile devices. As we move into the future it is likely we will begin to see new disruptive technologies in HEPs and advice, such as virtual reality.

While none of the products reviewed here included interfacing with gaming/virtual reality applications, there are already several products on the US market that deliver therapeutic-based exercise gaming interfaces. These were not included in this article because they do not provide home exercise and educational programs comparative to that of the paper based, index card type programs that are delivered traditionally as a part of therapeutic services. It seems likely that in the near feature developers of gaming based therapeutic interfaces and store and forward exercise programs will collaborate to provide both products in one.

Table 2 provides some potential benefits for each asynchronous feature. As new models of care emerge that maximize the use of cloud based software, mobile devices, smart devices and computers, we will likely see a complex integration of several types of products including gaming, texting, emailing, remote scheduling, exercise program prescription and client education that utilize both still picture video and haptic technologies all rolled into a seamless end-user experience. The usability of these hardware and software solutions in physical and occupational therapy assumes that all parties have access to a computer or handheld mobile device. In addition, practice administrators must consider the processes that these applications will be incorporated into, the usability of the product, and whether the benefits of their use outweigh the privacy and security risks.

WORKFLOW

Process can also be thought of as workflow. Although there are many innovative technologies and solutions available, only those that can be effectively merged with daily clinical workflows will result in long-term operational success (Ehrler & Lovis, 2014). Issues such as how client information is disseminated and EMR interoperability could potentially slow clinical processes and negatively impact clinical care interactions.

The current industry standard program allows for the dissemination of HEPs electronically with the creation of a PDF that can be emailed. This, however, creates extra time on the part of the therapist and hinders clinical workflow. Cloud-based solutions capture clients' email and allows for easy access by occupational therapists, physical therapists, and clients. With easy access may come some privacy and security issues, so a risk assessment is recommended using the checklist in Table 1.

Interoperability is another critical workflow issue. Store and forward content ideally should be integrated into the EMR that the therapist uses to record client encounters. EMR integration is hard to study with a wide-angle lens due to the variety of different EMRs and interfacing options. In our example, Cloud-based Solution A has built integration with an EMR by embedding their database of photographic and instructional content into the EMR. This is superior to scanning HEPs created with the store and forward application into the EMR, which results in more workflow steps for the clinician and support staff.

Process improvements can also be applied with thoughtful application of cloud-based store and forward technologies. By interfacing the daily exercise flow sheet filled out by the client into the EMR or portal allowing clients and providers to access ongoing data, both parties will ideally gain an improved understanding of cause and effect between program completion and progress with daily therapeutic goals pertaining to ROM, strength and functional performance.

USABILITY

Usability of store and forward applications must be considered when selecting store and forward apps and programs (Charness et al., 2010). This represents how relevant a technology is based on how easy it is for therapists and clients to interact with the application and its features and how likely users are to adopt technologies. Ease of access, navigability, feature relevance, and user acceptability are all examples of usability issues. Designing multiple strategies for assessment of usability will be important to successful identification of pertinent issues needed to successfully integrate healthcare IT solutions (Walji et al., 2014). Other examples of usability issues could relate to physical function, cognitive function, technology access and therapist/client willingness to adopt technology.

In our examples, the three cloud-based solutions highlighted in Table 3 offer clients and users remote access to their programs. To garner the greatest success, therapists and clients should have to complete as few steps as possible to use the program in a meaningful way. The current industry standard solution is solely accessible by the provider who emails a PDF and/or prints out the program for the client. This creates increased work on the part of the clients to track their progress and in the case of paper-based programs, may result in a higher rate of losing or misplacing the program than if it were in electronic form. However, technology access must also be considered. Without broad-band Internet access, it may be difficult for

clients and therapy providers to fully utilize all features offered by a store and forward application.

CONCLUSION

Returning to our case example, regardless of the store and forward application used, it will be critical for Mary to have detailed instruction on how to complete her rehabilitation program. A cloud-based solution may be desirable because of immediate access to the content, improved ability to capture ongoing data, and access to different media types (e.g., written, picture, video). However, caution should be taken to ensure that a cloud-based solution will be usable by clients, protect the privacy and security of their health information, and integrate well with clinical workflow -- thereby creating an efficient process. Cloud based store and forward technologies, strategically and appropriately deployed, can provide providers and clients with valuable tools needed to succeed in a value based healthcare model.

REFERENCES

Cohn, E.R., & Watzlaf, V. (2012). *Telepractice and informed consent: Readability of VoIP privacy policies*. Poster presentation at the national meeting of the American Speech-Language-Hearing Association, Atlanta, GA.

Charness, N., Boissy, P., Demiris, G., Krupinski, E. A., Lai, A. M., & Lopez, A. M. (2010). How human factors can influence the elderly in the use of telemedicine. *Telemedicine Journal and e-Health, 16*, 860–866. doi:10.1089/tmj.2010.9948

Ehrler, F., & Lovis, C. (2014). Supporting elderly homecare with smartwatches: Advantages and drawbacks. *Studies in Health Technology and Informatics, 205,* 667–671.

Rinehart-Thompson, L. (2013). *Introduction to health information privacy and security.* Chicago: AHIMA Press.

Schumer, C.E. (2014, August 10). *Press release - Schumer reveals: Without their knowledge, FITBIT bracelets & smartphones apps are tracking user's movements and health data that could be sold to third parties; calls for FTC to require mandatory "opt-out" opportunity before any personal data can be sold*. Retrieved from http://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-without-their-knowledge-fitbit-bracelets-and-smartphone-apps-are-tracking-users-movements-and-health-data-that-could-be-sold-to-third-parties-calls-for-ftc-to-require-mandatory-opt-out-opportunity-before-any-personal-data-can-be-sold

Sunyaev A., Dehling, T., Taylor, P., & Mandl, K. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association.* Advance online publication. doi: 10.1136/amiajnl-2013-002605.

U.S. Department of Health and Human Services [HHS]. (n.d.). *Health information privacy: For covered entities and business associates.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/

U.S. Department of Health and Human Services [HHS]. (2006). *Health information privacy: Frequently asked questions*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/250.html

U.S. Department of Health and Human Services [HHS]. (2007). *45 CFR 160.103*. Retrieved from http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-103.pdf

U.S. Department of Health and Human Services. (2013). *Health information privacy: Business associate contracts*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Walji, M. F., Kalenderian, E., Piotrowski, M., Tran, D., Kookal, K. K., Tokede, O., … Patel, V. L. (2014). Are three methods better than one? A comparative assessment of usability evaluation methods in an EHR. *International Journal of Medical Informatics, 83*, 361–367. doi:10.1016/j.ijmedinf.2014.01.010