Keeping Information Secure with Remote Users: Hospitals, HIPAA Restrictions and Telecommuting

Paul Heath
East Carolina University

July 24, 2014
On July 14, 2014, Newsweek ran a story covering the potential Long Island Railroad Strike (Wofford, 2014). The strike involved 300,000 Long Island Residents that made their way into New York City for work. The recommendation proposed by the MTA (Metropolitan Transportation Authority) for residents unable to make it into the city during the strike was to telecommute (The MTA network, 2013). Work trends over the past twenty years are not the same as they were in the age of our parents. Many people are not waking and making the routine commute into work anymore; instead they are getting up and heading over to the home office, their kitchen table or even the local coffee shop to begin their work day. Others might be sleeping in and starting their workday in the afternoon or evening. There are many ways to keep connected to the office today, which means one does not have to be at a certain place only open between certain hours. More and more, workers are free to be flexible with their day. This can all be credited to technological advances that make telecommuting and remote work (working away from the office) a possibility. Telecommuting is defined as using an Internet connection to perform one’s work from a remote location; a location removed from the physical space maintained and operated by one’s employer.

In 2013, 2.6% or 3.3 million employed United States citizens (excluding the self-employed) worked from home (Lister, 2013). Remote workers comprise a much larger portion of the population with, “over 17 million Americans relying on information technology to collaborate across distances away from a physical company office/headquarters,” *(Pierce, & St. Amant 2011, p.223). Telecommuting offers many advantages for today’s worker. For remote workers, individuals who routinely work in the field, such as sales representatives or home health care providers, it is a way to stay in contact with the office and keep informed of issues needing attention. For telecommuters, it offers the additional caveat of
being able to be employed without having to be on site. A good telecommuting program can be a strong recruitment tool for employers. It offers more of a favorable balance between work and off-duty activity for many. It cuts down on the costs of physically commuting to work, saving both time and money and allowing the employee to dedicate more energy to more personal and rewarding pursuits. For potential employees that might not consider moving to a densely populated part of the country there might be greater interest in positions if options include not having to travel into an office. This alone can pay employees in many saved hours of aggravation and expense; saving time as well as the costs associated with transportation and business attire (Beauchamp, 2014).

Telecommuting can help retain qualified employees if they need to move to another area and the nature of their work does not include having to be within driving distance of a certain location. Telecommuting is also environmentally friendly and cost effective for employers. Companies do not have to invest in utilities and on-site services for employees. There is no need for janitorial and coffee services if no one is there to benefit for the services. For the employees, telecommuting offers more flexibility in how they do their work and when they do their job. As long as the work gets done in a timely fashion most employers are not particularly strict about the time of day the work is completed. For home-based employees this adds more balance between completing work related items and home related tasks (Beauchamp, 2014).

There are potential problems related to telecommuting as well. For the extrovert used to interacting with people every day and people living away from family this can be big adjustment. These members may benefit from a remote access mentor. This could be another staff member that can serve as social support when in need. *(Koehne, Shih, & Olson, 2012)*
Sometimes telecommuters miss out on learning and modeling successful work habits from their coworkers and they miss out on some of the serendipitous creativity that grows out of collaboration with others. Still others have problems with discipline and getting their work accomplished in a timely manner, and some suffer from working from a home that has too many distractions (Beauchamp, 2014). Despite the challenges mentioned, however, two thirds of people still respond that they would like to work from home, and 36% would choose it over a pay raise (Lister, 2013).

A significant number of healthcare workers telecommute. According to U.S. Bureau of Labor Statistics, 14.7 percent of all healthcare workers work from home on an average day (Allard, M. & Lacey, J. 2009). As trends in telecommuting continue to grow for healthcare workers so do concerns with information security. This becomes an even more complicated arrangement because Healthcare workers have a specific constraint working with patient data. They are under obligation to make sure information remains secure and this obligation is enforced by the Health Information Portability and Accountability Act also known as HIPAA. (US Department of Health and Human Services, 2003).

**HIPAA and Information Security**

HIPAA, otherwise known as the Health Information Portability and Accountability Act was introduced by the U.S. Department of Health and Human Services in 1996. It is also referred to as the Privacy Act because it was introduced to keep patient information otherwise known as protected health information (PHI) protected. The law strives to strike a balance between keeping patient information protected and allowing it to be used where it is necessary. The type of patient information protected includes any data element that identifies the patient and
contains any information related to any evidence of specific physical or mental conditions, medical conditions being treated, or payments made related to care (US Department of Health and Human Services, 2003).

According to the United States Department of Health and Human Services OCR (Office for Civil Rights) *Summary of The HIPAA Privacy Rule* (2003) states there are six permitted uses and disclosures of information.

1. To the Individual - this is for the person served
2. Treatment, Payment, and Health Care Operations - this summarizes consults between other healthcare providers, payment from insurance companies and management and administration of the patient record.
3. Uses and Disclosures with Opportunity to Agree or Object – this includes disclosing information about the patient when it is deemed to be in the patient’s best interest such as notifying family of a patient being brought into the emergency room, listing their whereabouts in the hospital, or dispensing prescription drugs to someone acting on the behalf of the patient. The patient can agree or object to this if conscious.
4. Incidental Use and Disclosure – the result is a by-product of another permissible or required use or disclosure. It is an accident that happened even though all safeguards were in place to prevent the incident. For example, if someone over hears the doctor talking with the patient (Health Information Privacy, 2002).
5. Public Interest and Benefit Activities –
   a. Public Health Activities – preventing and covering disease
   b. Victims of Abuse, Neglect, or Domestic Violence
c. Health Oversight Activities – audits or investigations of healthcare

d. Judicial and Administrative Proceedings

e. Law Enforcement Purposes

f. Decedents

g. Cadaveric Organ, Eye or Tissue Donation

h. Research

i. Serious Threat to Health or Safety

j. Essential Government Functions – this includes military activities

k. Worker’s Compensation

6. Limited Data Set – a limited data set may be released as long as it removes patient
identifiers and the recipient arranges with the facility to follow certain safeguards
with the data.

(US Department of Health and Human Services, 2003). Any disclosure not mentioned above
would constitute a HIPAA violation. HIPAA violations are expensive and can include prison
time. Each compromised record can result in civil fines anywhere from 100 dollars to 50
thousand dollars with a cap of 1.5 million per year. Criminal penalties include prison terms from
1 to 10 years depending on the nature of the crime and the intent to commit (Wang, 2014). The
fines are levied by the type of violation whether it was a cause of oversight and the individual
was unaware of it or if there was any reasonable cause or willful neglect. If the party knowingly
entered into an act of fraud then the penalties become more severe and can include prison along
with high fines (Wang, 2014).
Security and HIPAA

HIPAA violations become part of the public record and are usually reported in the media. As an example, In May of 2014, Columbia University Medical Center and New York Presbyterian Hospital discovered an on-line breach of protected health information when someone in the vicinity reported finding medical information about their deceased partner by doing a routine Internet search (McCann, 2014).

The data breach at Columbia University Medical Center and New York Presbyterian Hospital occurred when a shared data network between both hospitals was comprised. An employee at New York Presbyterian Hospital tried to deactivate a personally owned computer server, which resulted in removing safeguards that left the health records of 6,800 patients unprotected and searchable on the Internet. The two hospitals involved reported the violation, which resulted in a combined fine of 4.8 million dollars; the biggest amount paid in history. In addition to the fines, both hospitals had to agree to, “a substantive corrective plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports,” (Friedman, 2014).

The Columbia University Medical Center/New York Presbyterian Hospital incident mentioned above is not an isolated case. There are many tales of health agencies being fined millions of dollars for stolen unencrypted USB hard drives or laptops. Fines have also been levied for offences such as backup tapes disappearing and photocopiers returned without erased hard drives (Wang, 2014). The incidents reported strongly suggest the need for effective security protocols to protect patient data and ensure that healthcare organizations remain effective providers of their primary services.
According to the Ponemon Report on Patient Privacy and Data Security (2014) released in March 2014, all is not bleak. Some of the key findings of the study showed data breaches have slightly decreased; 90% of the hospitals surveyed stated that they had at least one data breach over the past two years with 38% reporting they had five or more data breaches. The cost of these data breaches have decreased along with the severity of each offense. On the down side, criminal attacks have doubled since last measured (Ponemon Insitute, 2014). The report also referenced looming threats with the Affordable Care Act based on data exchanges with insecure websites, databases, and health exchanges. Still, to date the biggest threat to Protected Healthcare Information is employee negligence. Healthcare providers rely too much on policies and procedures to regulate how employees interact with the data but this is not enough. More technological and physical safeguards need to be in place to help employees protect themselves. (Ponemon Insitute, 2014).

**Policies and Safeguards**

Reliable reports of cybersecurity problems can serve as cautionary tales, prompting those responsible for an organization’s security to re-examine existing policies and safeguards, and to determine what policies and safeguards need to be implemented in preparation for the possibility of increased telecommuting. Given that so many people are working remotely, there must be a correct way to work productively outside of the office network. The most effective methods of making remote relationships work are a good telecommute policy and appropriate safeguards.

A telecommuting policy is a set of guidelines that an employee must adhere to if he or she wants to work remotely. The first step in creating a good telecommuting program is deciding which employees and which type of work is right for telecommuting. A manager
should select employees that have a good track record of producing quality and valued work. The candidate will need to be one that does not need as much office supervision. Most healthcare careers can involve some amount of telecommuting time. However, those positions in which the individual needs to provide patient care, or direct supervision of patients or staff, or facility care (e.g. custodial work) would have to remain onsite. From the author’s perspective as a hospital employee for over a decade, ideal healthcare jobs eligible for telecommuting include administration, information technology, healthcare coding, insurance processors, nurses using smartphones, and visiting home health workers. A good policy should establish the number of hours the employee will work from home and from the office (if applicable) and both means of communication and contact availability. Safety, security and technology should also be the cornerstone of a good telecommuting policy. When staff members work from home there is always a question of who is responsible for keeping the workplace safe and who is accountable for an unsafe environment. For this reason, the policy needs to specify who is responsible for keeping the work environment free from hazard and give the employer the right to inspect the property to make sure these guidelines are being met. Security and technology also need to be part of the policy (Grensing-Pophal, 2005).

Good security and technology practices include employee behaviors that can be taught and enforced by technology. The University of North Carolina at Chapel Hill gives their employees the following guidelines to help keep data secure (University of North Carolina at Chapel Hill, 2013-14):

- Do not allow others to access one’s work computer
- Keep one’s personal passwords and logins secret.
• Pick strong passwords with at least 8 characters with a combination of letters, numbers and characters.
• Change one’s passwords every 45-90 days to keep hackers from gaining access information.
• Make sure one has a screen saver that will lock when the system is not in use.
• Avoid storing patient health information on external storage units - if that is unavoidable make sure one uses encryption and data is stored only temporarily for the transporting and then deleted. (University of North Carolina at Chapel Hill, 2013-14).

Mobile devices are an increasing threat to unauthorized disclosures of patient data. They store a record of data exchanged in the mobile device memory and on the SIM card. They are also small and portable making them easily misplaced, lost or stolen (Barrett, 2011).

**Bring Your Own Device, or BYOD**

More and more employees are bringing their own mobile devices to work – a phenomenon known as BYOD (Bring Your Own Device). The use of smartphones alone has been credited with increasing productivity by 250 hours per year, *(Yun, Kettinger & Lee, 2012)*. They have also been tagged with maintaining an “Open Door Policy” since these devices can be used 24/7 for a means of delivering information and communications *(Yun, Kettinger & Lee, 2012)*.

The problem with these mobile devices lies in the fact that they are usually the property of the individual and configured by the individual often not having the type of software needed to be secure from external threats. The main threats associated with the use of mobile devices include insecure web browsing, insecure wi-fi usage, lost or stolen devices, corrupt application on device and lack of security patches (Barrett, 2011).
According to John Chirillo of More Direct, a PC Connection Company (n.d.), best practices for personal mobile devices include:

- Use some type of authentication like a password
- Use encryption
- Install and activate wiping and/or remote disabling
- Disable File sharing
- Install a firewall
- Install security software
- Keep security software up to date
- Research apps before downloading
- Keep mobile device secure
- Use adequate security to send or send email over public networks
- Delete all store health information (Chirillo, n.d.).

**Data Security**

Shred documents no longer needed to perform the work task and try to go paperless as much as one’s institution will allow. If documents are stored make sure they are stored in a locked filing cabinet behind a locked door. Only send the amount of information necessary for the task at hand. Strip out any data elements that are not necessary. In the case of any breach, misuse or possible breach of information security regarding patient related information be sure to promptly contact one’s supervisor and one’s organizational security information manager. Make sure antivirus and anti-malware software is up to date (Chirillo, n.d.).
Secure Remote Connection: Virtual Private Networks

Securing equipment and protecting accounts is a great practice for preserving hospital data, but for the healthcare worker that needs to transmit and access large amounts of secure data and access healthcare records a secure connection needs to be established between the user and the place of work. The best type of network account for access is creating a VPN (Virtual Private Network) based on the Secure Socket Layer technology. This provides the highest level of security needed for healthcare access (Kawamura, n.d.).

“SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser,” (Rouse, 2009). The advantage of SSL VPN is that it can be used with any standard web browser, which means it does not have to rely on a standard VPN set up where software has to be installed and maintained on one machine (Rouse, 2009). A VPN allows for use of a public network or infrastructure to connect to a private network using a SSL protocol to encrypt on either side thus making it a secure data exchange. SSL protocol uses two types of set-ups. The first is portal because it uses a single connection to allow the user to connect to multiples services of the organization. With this type of setup the user establishes a connection to one single webpage that has links to several services that a user might need. The second type of SSL set up is often referred to as tunnel SSL because it uses a tunnel that is running under the SSL (Frankel, Hoffman, Orebaugh & Park, 2008). Tunnel SSL connections allow the user to connect to multiple applications and services even the ones that are not web based thus simulating logging into your desktop at the office.
Discussion

Based on the research reviewed above, one can identify three main groups of people involved in creating a successful telecommuting program; administrators, Information Technology (IT) staff, and those employees who are working remotely.

Administrators are the ones in charge and the ones with the authority to create teams to support telecommuting and get the buy in from staff to support the policy. They need to be responsible for setting and reviewing the telecommute policy to make sure it is still effective in achieving the objectives of the organization and still meets the standards of security that are necessary for doing business. For the sake of the organization, they need to be constantly looking for ways to make sure the appropriate and least amount of data gets into the hands of their employees so that they can do their jobs appropriately.

Information Technology staff accounts for the success of a good telecommute program. They need to be comprised of teams with the appropriate skills to deliver information in a secure manner. They need to be on top of the latest threats to data, the latest technologies to securely deliver data and any updates in networking technology equipment or protocols that would make sure data is protected. They need to assist in the policies governing devices, software and training of staff. Equipment used by employees needs to be tested and set up to make sure it has encryption, locking security screens, antivirus software and meets the standards created by the organization. They also need to play a key role in training staff about best practices for protecting data whether that be through on-going email communication, annual modules or training sessions.

Human error comes up in many of the readings as the biggest threat to information security and HIPAA violations. Employees need to use best practices when interacting with
data. Home offices should be treated more like an office created by an employer.

Telecommuting is not another means of childcare and employees should not be dividing their attentions between work related and non-related activities. They need to make sure they are practicing all the safeguards set up by their employer. When in doubt about any breach, policy or practice, they need to be in contact with their employer for further training or counsel.

Recently, the author attended a friend’s birthday party and was discussing cyber security and HIPAA violations with a fellow partygoer. He stated that he disliked that he could not email other facilities with any identifying information for advice on placement or care of a patient. Where we are today with remote access, telecommuting and cyber security is in response to the threats that face our data and the cost involved in making mistakes with patient data. As more protocols are developed and more networking technology exist to make data more secure, we may see more exchanges of data across many more networks. Polices and safeguards will still be a crucial part of data protection, but more secure exchanges of data will decrease the risk for organizations and increase the practice of telecommuting. In twenty years, future generations will probably be writing papers about how different their work experiences are from 2014.

Conclusion

As noted in the introduction, Telecommuting continues to grow in popularity and public recognition. Healthcare involved in telecommuting have special considerations due to HIPAA. This review of the literature and discussion of possible policy is just a beginning. Further research and review is needed to develop the best strategies keeping patient data secure and create the most productive environment for telecommuting healthcare workers.
References


