Patient, Provider and Payer:

Why it is in everyone's interest to move patient health information out of the premise and onto the cloud

V1.1
11/3/2017

ABSTRACT

The security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) often lead providers to an overly-restrictive view with regard to the handling of protected health information (PHI). With the advent of electronic protected health information (ePHI), this overly-restrictive view has spilled into the cyberdomain, particularly with regard to on-premise vs. "cloud" storage and use of ePHI.

Introduction

In 1996 Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). For the purposes of this paper the important provisions of HIPAA are:

1. The establishment that protected health information (PHI) is the property of the patient, not the provider.
2. The establishment of administrative, physical, and technical safeguards that a covered entity[1] must implement to ensure protection of patient privacy when handling PHI.
3. The requirement that covered entities must not withhold or restrict the use or transmission of PHI when that PHI is material to the treatment and wellbeing of the patient.
4. Civil and criminal penalties for violations of any of the above.

Items #2 and #3 are generally defined in the portions of the HIPAA act defining the HIPAA "Privacy Rule" and "Security Rule." In particular, the Security Rule directly addresses the issues around electronic PHI (ePHI).

Collectively these provisions encompass HIPAA's "dual mandate." The dual mandate is:

1. A covered entity must take reasonable steps to protect PHI when PHI is within the covered entity's stewardship
2. A covered entity must not withhold the use, storage, or dissemination of PHI when that use, storage, or dissemination is in the interest of the patient

[1] A "covered entity" is a health plan, health care clearinghouse, or health care provider. In addition any business associates (identified by having a business associate's agreement (BAA) with a covered entity) are also considered covered entities.

Before going on let us define, as precisely as possible, what constitutes PHI. While there are many definitions floating about, including definitions that enumerate each possible type and domain of data that could constitute PHI, the simplest and most direct definition is that used by the Center for Medicare and Medicaid Services (CMS):

> *PHI is any information that could be used to infer the past, present, or future provisioning of medical care to an individual*

Let us use two examples of the above to help illustrate the concept:

1. A provider, such as a large hospital, sends out a bulk email to every patient it has seen. The wording in the email asks the patient to participate in a survey

   This is PHI because each of the emails contains the email address of the recipient. Someone who came into possession of any of those emails could infer that the recipient had received medical care from that provider.

2. A dataset containing nothing but the ages of patients treated at the provider and the zip code within which the treated patient lives.

   This is PHI, particularly if some of the ages are sufficiently high to identify an individual. For instance, if in zip code 94117 it is disclosed that a 102 year old individual was treated then it could be possible to individually identify that individual (there are not many 102 year old individuals in any zip code)

HIPAA's First Mandate: Protect Health Information

The Risks Are Real

Let's concentrate now on the first part of the HIPAA dual mandate: the requirement to safeguard protected health information. What consequences have arisen from the inappropriate disclosure of PHI?

As of September, 2017 the US Department of Health and Human Services' Office for Civil Rights (OCR) has:

- Received over 165,000 HIPAA complaints
- Determined that roughly 50,000 of those complaints had merit
- Investigated and resolved over 25,000 of those cases
    - Roughly 23,000 cases were resolved with early intervention by OCR
    - Imposed $73 million dollars in fines and settlements related to 52 of the remaining cases

Where are the violations occurring? According to OCR the most common types of covered entities required to take corrective action are (in decreasing order of frequency):

- Private Practices
- General Hospitals
- Outpatient Facilities
- Pharmacies
- Health Plans (payers)

What types of violations? Again, in decreasing order of frequency:

- Impermissible uses and disclosure of protected health information
- Lack of safeguards of protected health information
- *Lack of patient access to their protected health information*
- Lack of administrative safeguards of *electronic* protected health information (ePHI)
- Use or disclosure of more than the minimum necessary protected health information

Civil and criminal penalties associated with the inappropriate disclosure of PHI are not the only form of harm that befalls covered entities. Of perhaps even greater consequence to an organization are the impacts of negative media coverage surrounding a PHI breach.

See Appendix A for a meta-list of the most notable headlines of 2017.

On-premise: Security Through Obscurity

Is data "in the cloud" inherently less secure than if the same data were stored "on premise," say within a provider's own data center? Illustratively, a recent discussion on the topic elicited this comment: "[there is] a fundamental bias many of us have — the belief that data 'within my purview' (i.e., on-premise) MUST BE safer that data that I entrust to others. And incidents like the Equifax breach further strengthen this bias."

This is a compelling argument and one used to justify the building of not only electronic walls and walls around buildings but also walls around entire nations. Its appeal is simple and digestible. It is also flawed for the simple fact that there are only two kinds of walls in the world: those that have been breached and those that will be breached.

A review of case histories reveals that, at best, information security breaches are currently divided half and half between breaches that occurred "on premise" vs. breaches that occurred in cloud-based systems. This is for all types of systems across all industries, not just healthcare.

In healthcare the numbers are much worse. Overwhelmingly, where ePHI is inappropriately disclosed, it is disclosed from an on-premise system. Appendix A of this whitepaper enumerates that, of the thirty-six major health-care breaches in 2017 (according to the publication HealthcareIT), not a *single* breach occurred on a cloud-based system.

Much of this is due, of course, to the fact that the vast majority of ePHI is still stored in on-premise systems, not cloud. Nonetheless, in each case the breach happened because an assumed secure wall was not secure. Let's give one example of how that might happen:

Joe, who works for Amalgamated Memorial Mercy Health, arrives at work one morning and discovers a USB flash drive lying on the ground in the parking lot. Being curious, Joe puts the USB drive in his pocket and heads in to work.

At his desk, Joe remembers the USB drive and takes it out of his pocket. We know he's curious so, naturally, he puts it in his computer to see what is on it. When he does, it appears to just be a collection of someone's vacation pictures. What Joe doesn't know is that the USB drive also had a virus on it. That virus infected his desktop computer and has now established a connection with a computer outside Amalgamated's firewall. The outside computer is now controlling Joe's computer. Since Joe's computer has access to Amalgamated's EHR system, all of Amalgamated's patient data is now on its way to a foreign country where blackhats will hold it for ransom until Amalgamated pays them ten million dollars (in bitcoins).

(p.s. True story)
(p.p.s. The Equifax breach was also an on-premise breach)

The Cloud: Defense in Depth

Another reason often given for the superior security of on-premise ePHI is that each individual organization, provider in our case, presents a smaller target than a large cloud/SaaS provider such as AWS or Salesforce. In other words, hackers aren't going to bother with trying to break into a thousand separate provider's networks when they can just set their sights on Salesforce and hit the motherlode.

However, there are very sophisticated and highly distributed penetration systems that are capable of attempting to breach the firewalls and other defenses of tens of thousands of organizations simultaneously. This makes every organization, regardless of its size or visibility, equally subject to attack.

While it may seem counterintuitive, all evidence points to the reality that cloud solutions are more, not less, secure than on-premise solutions. Although action in healthcare as an industry is lagging in this regard, many industries – including high security industries such as finance – are shedding on-premise security liability via a migration of their data to the cloud.

Why do cloud-based solution offer higher levels of security over on-premise systems? The driving reason is motivation. A cloud service provider's entire business depends on customer's confidence that their data will not be compromised. A breach of customer data at an organization that holds itself out as a cloud service provider carries the very serious risk of that organization going out of business.

All organizations are equally motivated to prevent their data from being breached. However, some organizations are more equal than others. Specifically, if your entire business depends not on keeping your own data safe but on keeping your *customer's* data safe then it can be said with authority that not only are you motivated but that you are *existentially motivated.*

A cloud service provider is acutely aware that they are high-value targets for cyberattack. Because of this they invest heavily in policies, procedures, personnel and technology to ensure that no attack is ever successful. Again, it is an existential issue for the business.

All of the major cloud-infrastructure providers (Amazon, Microsoft, Google) and the cloud-service providers, such as Salesforce, employ vast arrays of technology to defend against cyberattack. These include the traditional tools and products, the kind a typical large provider may use in its on-premise systems. But they also include sophisticated, proprietary, systems using artificial intelligence, statistical analysis, packet sniffing, etc. to actively, automatically, and constantly monitor their systems. Providers do not have those tools and defenses on-premise.

Likewise, the sheer number and qualifications of personnel with cybersecurity responsibility at any of the cloud providers simply dwarfs the number (if not the qualification) of persons with equal responsibilities within a provider's organization.

HIPAA's Second Mandate: Make Health Information Available

The opportunities are boundless

We've discussed the implications of the first part of the HIPAA dual mandate: the consequences of a PHI breach. And which environment, on-premise or in-the-cloud, is inherently more secure against a breach. Now let us turn to the second part of the dual mandate: access to ePHI.

Background

In general, providers tend to over-emphasize the protection requirements of HIPAA while under-emphasizing the use and dissemination requirements of HIPAA. In fact, most providers are unaware that HIPAA requires providers to not only protect PHI (including ePHI) but to also put PHI/ePHI to use in the patient's interest.

Furthermore, providers tend to be culturally unwilling to accept that patient records belong to the patient, not the provider. Attitudes regarding access to and interoperability with health records among the various vendors of electronic medical record (EMR) and electronic health record (EHR) systems only reinforces the provider's reluctance to "let go" of PHI.

The reason for that is as simple as it is unacceptable. For both providers and EMR/EHR vendors, the reluctance to relinquish control of PHI is driven by economics. Providers fear that if they allow PHI to leave their premises, then so potentially could the patients. For providers, PHI portability equates to patient portability. For EMR/EHR vendors, PHI portability equates to system portability. As long as a patient record cannot be easily extracted from the vendor's system is as long as the vendor's system won't be replaced by a competitor's.

While HIPAA enforcement actions stemming from the inappropriate disclosure of PHI are well known, what is generally not well known are the HIPAA enforcement actions stemming from the inappropriate *withholding* of patient health information. In fact, according to the Department of Health and Human Services, actions stemming from "lack of patient access to their protected health information" is the *third most common type* of enforcement action.

Things are changing

Above we described what has traditionally been the attitude among providers regarding access to patient health data. And, from the provider's perspective, there is a certain understandable justification behind the attitude. But there are emerging reasons where, again from the provider's perspective and in the provider's interest, that attitude should change.

The United States is in the beginnings of a transition away from its unique fee-for-service healthcare model and towards the fee-for-outcome model used in the rest of the world. Under fee-for-service, providers are paid to treat sickness. Under fee-for-outcome, providers are paid to sustain wellness. To drive the point home: doctors and hospitals make money when people

are sick under fee-for-service. Under fee-for-outcome doctors and hospitals make money when people are healthy. It is not hard to understand how the perverse financial incentives inherent in fee-for-service can have hidden effects on the quality of healthcare in the United States.

Another way to frame the issue is to recognize that fee-for-service focuses on action. It is quantitative and transactional in nature. Fee-for-outcome focuses on quality. It is qualitative and dialectic in nature.

As William Deming counterintuitively observed: a qualitative focus results in improvement in quality and a decrease in costs. That's the bottom-line that providers should embrace. Under fee-for-service it made financial sense to sequester health records on-premise. Under fee-for-outcome it makes financial sense to put them in the cloud. Let's examine that statement.

Including the role of Information Technology in healthcare

Under the fee-for-service model the use of Information Technology (IT) in healthcare has been limited to a few functions. The functions are operational in nature and primarily centered around patient registration, patient scheduling, and payer billing. In fact, nearly all of the major so-called electronic health record (EHR) systems available today were developed from earlier practice management systems (PMS) whose functions were limited exclusively to scheduling and billing.

While they may now be marketed as one-stop systems for everything from clinical records to patient portal access to population health management, scratch the surface of any major EHR system and you will find the DNA of a cash register.

Any provider wishing to survive and thrive in a fee-for-outcome environment will recognize that thriving requires a fundamental reassessment of the role and expanse of information technology in their organization.

Under fee-for-outcome, the role of IT in healthcare must move out of the backoffice. The most fundamental asset of IT in the future centers around its role in communication. That is communication between patient and provider, communication between provider and payer, communication between everyone. The future in healthcare is as it is everywhere else: social media, the expansion of the definition of community, and a technology-boosted increase in the ability to know about others and to use that knowledge toward action guided by empathy.

Quality is a goldmine and technology is the equipment that can be used to mine it.

Speaking of money…

The great tragedy in the United States are these facts[2]

- The United States has the highest per-capita costs for healthcare, by far, of all its peer (OECD) nations
    - Almost entirely due to the fact that providers in the United States charge far more for a given procedure than do providers in the rest of the OECD
        - Lack of "single payer" monopsony buying power.
- The United States has the poorest outcomes and worst-performing health care system in the OECD.
    - Disparity between money spent on encounter-based medical care vs. money spent on social programs, compared to the OECD norm.
- Not surprisingly, patient satisfaction with the health care system in the US is lower than the patient satisfaction in the other OECD countries. Drivers of this dissatisfaction include:
    - Long wait times to see a physician for non-emergency situations
    - Rationing (i.e. access to health care and the cost of health care)
    - Poor outcomes, including poor patient/provider relationships

This is clearly an unsustainable situation and one that plays out now almost daily in the news within the US. This unsustainability is the primary driver of the transition from fee-for-service to fee-for-outcome. The payer population[3], in particular the largest payer (the Federal Government), is now beginning to tie payment to outcome.

There are various ways of tying payment to outcome, including self-reported quality metrics by the providers. One set of those metrics involves the access to and utilization of electronic health records by patients of the provider. Other outcome factors emerging are the ways in which patient health records are used by the provider to predict population health risks and trends, to identify lifestyle and co-morbidity issues among the patient population, etc.

Enabling any of that means opening up patient records to consumption and analysis by a disparate array of systems, from different vendors each capable in their own specific domain of expertise. In other words, communication of and about patient records by those systems.

Providers who cannot deploy the systems necessary to bring together patient data irrespective of its source, to monitor quality factors, to do complex population health analytics, to support telehealth, to support patient engagement and empowerment are providers who are going to increasingly find it hard to get paid.

---

[2] Data from the Commonwealth Fund, World Health Organization, Kaiser Family Foundation and Organization for Economic Co-operation and Development (OECD)

[3] The United States is also unique within the OECD in that it does not have some form of single-payer/universal coverage system. The lack of such a system is the largest single contributor to the high cost of health care in the United States.

Speaking of patient data…

Another word for communication is interoperability. Most industries, from transportation to finance to eCommerce and beyond have a rich set of robust standards and technologies that facilitate interoperability – the exchange of information between disparate systems.

Given its size as a portion of our economy, healthcare is unique in that it alone does not possess any rich set of standards or infrastructure to promote interoperability. What standards it does have, such as the HL7 standards, are hopelessly unstructured and/or arcane to use beyond a few basic functions.

Talking all the time

In stark contrast to the situation in healthcare, the interoperability ecosystem in the cloud is comprehensive, secure, and enormous. Standards such as SOAP, REST, OAuth, XML, JSON, etc. abound and are used daily to support billions of interactions between disparate systems. Some of those systems, such as the military and financial, have security requirements which dwarf those of HIPAA.

As IT expands and is marshalled in support of healthcare's qualitative mandate, interoperability becomes an absolute requirement. Initiatives such as patient mobile access to their data, care transition, patient relationship management systems, population health, chronic care management, etc. all require the support of patient health record interoperability and availability that on-premise solutions cannot provide.

But that are trivial in a cloud-hosted environment.

Appendix A – Notable Breaches of 2017

(HealthCareIT, October 2017)

1. Arkansas Oral Facial Surgery Center. 128,000 patients. On-premise.
2. Augusta University Medical Center. # of patients unk. On-premise (phishing attack)
3. Medical Oncology Hematology Consultants. 19,203 patients. On-premise.
4. Kaleida Health. 744 patients. On-premise (email hack)
5. Mid-Michigan Physicians Imaging Center. 106,000 patients. On-premise.
6. St. Mark's Surgery Center. 33,877 patients. On-premise.
7. Pacific Alliance Medical Center. 266,123 patients. On-premise.
8. Plastic Surgery Associates of South Dakota. 10,000 patients. On-premise.
9. Anthem BlueCross BlueShield. 18,000 patients. On-premise.
10. Women's Health Care Group of Pennsylvania. 300,000 patients. On-premise.
11. Peachtree Neurological Clinic. 176,295 patients. On-premise.
12. UC Davis Health. 15,000 patients. On-premise.
13. Bupa global health insurance. 108,000 customers. On-premise.
14. Indiana Medicade. 1.1 million. On-premise.
15. Cleveland Medical Associates. 22,000 patients. On-premise.
16. Airway Oxygen. 500,000 patients. On-premise.
17. Feinstein & Roe MDs; La Quinta Center for Cosmetic Dentistry. 6,000 patients. On-premise.
18. Washington State University. 1 million patients. On-premise.
19. Torrance Memorial Medical Center. Unknown. On-premise (phishing attack).
20. Molina Healthcare. 4.8 million patients. On-premise (patient portal)
21. New Jersey Diamond Institute. 14,633 patients. On-premise (EHR server)
22. Harrisburg Gastroenterology. 93,000 patients. On-premise.
23. Bronx-Lebanon Hospital Center. Millions of patients. On-premise (backup server)
24. Aesthetic Dentistry and OC Gastrocare. 180,000 patients. On-premise.
25. Children's Health Records. 500,000 patients. On-premise.
26. Lifespan. 20,000 patients. On-premise (laptop theft).
27. HealthNow Networks. 918,000 patients. On-premise of a non-covered entity (BAA failure)
28. ABCD Children's Pediatrics. 55,000 patients. On-premise.
29. Washington University School of Medicine. 80,000 patients. On-premise (phishing attack)
30. Metropolitan Urology Group. 18,000 patients. On-premise.
31. Denton Heart Group. Unknown. On-premise (stolen hard drive)
32. Brand New Day. 14,000 patients. On-premise.
33. Singh and Arora Oncology Hematology. 22,000 patients. On-premise.
34. Verity Medical Foundation-San Jose Medical Group. 10,000 patients. On-premise (website hacked)

35. CoPilot Provider Support Services. 220,000 patients. On-premise (website hacked)
36. Indiana-based Cancer Services. Unknown. On-premise.