Abigail Busath

Individual Research Paper: Intermountain Healthcare

When Machines Decide Praxis Lab

University of Utah

November 17, 2016

Intermountain Healthcare is a non-profit healthcare organization that serves communities as the largest healthcare organization of the Intermountain West. The organization began in 1975 after the Church of Jesus Christ of Latter-Day Saints, who operated around 15 hospitals in the intermountain community, decided to donate these hospitals under the condition that a "not-for-profit organization would be formed to operate the hospitals on behalf of the communities they served." Since its formation, Intermountain has quickly risen as one of the nation's leading healthcare organizations, with top of the line research and technological advances, such as Life Flight, with recognition at the federal level for excellent research and patient care, and has even been in the international eye when it was the official healthcare provider for athletes in the 2002 Salt Lake City Winter Olympic Games. The Intermountain system operates 22 hospitals throughout Utah and Idaho, and has some 37,000 employees.

As a leading healthcare system, Intermountain has a large data system to maintain and interpret to both contribute to research and optimize patient care. One of the leaders of the data team is Lee Pierce, whose title is Chief Data Officer at Intermountain Healthcare, who was kind enough to interview with me about the practices and policies of Intermountain's data collection.

Lee has worked at Intermountain for over 21 years, specializing in healthcare IT, and currently focuses on the department of Data Management and Analytics. In his own words, his responsibilities include defining data and the quality of data practices. He also coordinates how data is used in decision making, while overseeing a team of 80 employees that help to make predictive models that research how the medical experience can be improved.

After a brief introduction, Lee and I transitioned our conversation to the data. Firstly, I posed the question; what data does Intermountain collect, and who specifically do they collect it from? Lee explained that data exists and is collected in every business and clinical process in the company. Information about patients could range from “insurance, patient history, clinical conditions, symptoms, family members, and family history”. Employees of Intermountain have data on who they are, what their job is, what their responsibilities are, and who their supervisor is collected in the Intermountain data system. Other members of the patient’s health plan, such as their insurance provider have data collected from them as well. For example, Select Health, as the primary insurance provider for Intermountain Healthcare, is part of the health plan. Data collected from Select Health includes the patient’s primary care provider, every time they are treated, the bill that is sent to the insurance company, how much things cost and what treatments they receive. Every process that happens in an Intermountain Healthcare facility has a data trail that is collected and interpreted by Lee’s data team.

Next we talked about the methods Intermountain uses to collect this data. Lee explained that there are many ways they can obtain the information, but he highlighted a few key methods. Mostly the clinicians such as doctors and registrars that ask clients questions prior to appointments and procedures will input the data in to the online system. Also used are surveys sent electronically to personal devices or a kiosk at specific facilities. Less used methods are personal health devices like iPhones and fit bits, which are constantly collecting data on their owners can be made available to clinicians with permission. Also available to clinicians with permission are social media posts and information that can also be analyzed to promote patient care.

Naturally I had to ask why Intermountain collected this data. Lee responded that the data is collected “just to be able to run the business of healthcare.” A scenario he described involved patient billing. He explained that when Intermountain provides a service to a client, data on the client and the treatment provided is collected and interpreted so the company can receive payment for that service. But more importantly, data is collected to ensure that Intermountain lives by their mission to help people live the healthiest lives possible. By collecting patient data such as their history and condition, doctors and researchers are better able to determine courses of action that will help treat their patient’s optimally. By statistically determining the likelihood of a patient’s reaction to certain treatments against their specific symptoms, healthcare providers are able to not only care for the condition, but also prevent the patient from being re-admitted to the hospital. Statistics retrieved from patient data also help to determine preventative measures that at-risk people can take to ensure they are not infected, effectively keeping them out of the hospital and saving them a lot of time and money.

After our discussion about data collection, I posed a few questions to Lee about how Intermountain uses the data that they collect from patients and employees- and particularly how often the data is accessed and used. Lee said, “Data is the lifeblood of a business. It is constantly flowing throughout our systems, aiding us to make effective company decisions that keep the business running. Now, this is a hard question to answer, because is *your* personal data being used constantly? I would say no. It comes and goes like you would to a doctor’s appointment. When you are here, we pull up your data to make effective decisions for *you*, but when you leave, we’re not really using it anymore.” I thought that this was an interesting response, because some people may take his statement to mean that their personal data is easily accessible, and when you're not at a facility, the information is just floating around somewhere in the ether, waiting to be read by somebody. This prompted a few more questions about data storage and security.

First I led off with, how is all the data stored by Intermountain? Lee explained that the data can be stored in either databases or data files. The difference between the two is basically that databases store *organized* information, while data files can just store data; both are regular methods of data storage. "For every data system [like patient histories or billing information]," Lee explained, "There is a database or data file system that the information is stored in." For example, the electronic medical record has a separate base that it's stored in, as does the laboratory that processes lab specimens, as does the billing system, as does the employee information system, as a way to organize the vast amounts of information Intermountain has. Though the different systems are stored separately, they can then be extracted and brought together in what Lee calls the "enterprised data warehouse" where individual data points can be "linked together and used to analyze as combined data for patterns that help to create insights that contribute to better health and company decisions." "Better decisions are made with data than without data," Lee added.

With this new revelation about data storage, another question came to mind. "How long is the data stored for?" I asked Lee. "Is there a limit to how long you can store data?" I myself have a personal history with Intermountain Healthcare, as my mother works at LDS Hospital, and I have personally seen storage rooms with paper health records that date back many years. I was curious then, to hear Lee's response, because for a long time I have wondered how long the system can hold onto these physical records, especially when they constantly add more as the years go on, and they can’t possibly have enough space to keep every record. Lee didn’t disappoint. He explained that data can take on different formats- physical (like the papers I’ve seen) and electronic, which is what he works with. Previously (before electronic health records became so prevalent) Lee clarified that paper records had regulations on how long they could be stored, which was usually up to 7 years after the patient was seen. Now, however, that data has become less expensive to store, many of these paper records have been scanned into the system to be used for research as picture images, though this is a long and meticulous process to find. Lee said that, “data lives on, but is not deleted because it is valuable. There are some policies we have that require us to clean out our systems, such as clearing out email every six months. But ultimately there isn’t a reason to delete data unless there is a legal or regulatory reason the data needs to be deleted. There are many insights and decisions to be made using our data.”

With such precious information- and so much of it- I had to ask Lee what kind of security measures are in place to ensure data safety. He started out with explaining that “data and Information Systems security is a big deal and will continue to be a big deal to Intermountain.” He assured me that there is a team of 50-60 individuals who are dedicated to manage the Information Systems and actively combat cybercrime. This Security Operations Center (SOC) is constantly monitoring threats, data movement, attempts by hackers to break into the systems, and regulating cybercrime. He explained that years ago, an initiative was implemented that installed special software on every Intermountain laptop that encrypted the hard drives. This made it so that thieves couldn’t just take the hard drives out to access patient data. The encryption means that without a password or identification, you can’t access the files in the drive, effectively limiting someone who isn’t an Intermountain employee from viewing patient files. Lee also explained that Intermountain has in place firewalls and 2 factor authentication security that also protect data files from outside forces. 2 factor authentication refers to the requirement that in addition to a username password, employees must have a 2nd form of identification to make their way into a system.

On that note, I decided to ask Lee to put in perspective just how difficult it is for hackers to breach the Intermountain Information System, and if breaches are common. Lee assured me that it is extremely difficult to breach the system from the outside, simply because of the team in the SOC who are monitoring the system continually, and the many security measures that are put in place on the file systems. He said that "normally when you hear about a data breach, it has come down to an employee who hasn't followed procedure correctly- whether that be they left their monitors open and logged in, or they've shared their passwords with someone else, or simply have made their information available to others who use it to compromise the system." He explained that there are extensive measures and policies that employees have to go through to ensure they understand and act appropriately so that their information is safe- procedures which I can attest to are very effective.

Finally I asked Lee who exactly has access to the stored data? Is it just employees or can anyone obtain "permission" to read the files? He said that there are protocols that Intermountain follows when dealing with access to patient data. Data analysts that work for Intermountain Healthcare can obtain access to analyze data sets to make company decisions. Researchers are also granted access after following legal protocol to request data. Ultimately, though, Lee said that "to get access to data, it primarily has to be for the purpose of running the business efficiently and making health decisions. The accessibility is tightly controlled to ensure that no data that isn't needed to be used is accessed." In short, if it's not a relevant part to your job, Intermountain isn't going to grant you access.

Thus we wrapped up the conversation and thanked each other for a pleasant chat. I had to hand it to Lee- he was very thorough and helped my understanding of medical data collection and storage greatly.

To corroborate Lee’s description of Intermountain Healthcare’s data use and collection, I did some more research on the company website. They have a page that describes their concerns for patient safety, lists the rights of the patient in terms of what they can request about their data, reasons they use patient data, and the rules when it comes to sharing patient data. Overall Intermountain takes patient and employee information very seriously.

Intermountain’s website page that discusses patient rights to Health Information Data contains a list of requests patients are allowed to make regarding their health information. These rights include:

- Inspect and get a copy of your medical or billing records (including an electronic copy if we maintain the records electronically), as allowed by law, usually within 30 days of your request.
- Request in writing that restrictions be placed on how your health information is normally used or shared for treatment or other purposes.
- Request an accounting of when your identifiable health information is shared outside of Intermountain for a purpose other than treatment or payment, for example.
- Receive notice if we or our business associates have breached the confidentiality of your health information.
- Request in writing that your health information be amended if you think that information is in error.

Though these rights are just a few of the total listed, they represent a company that is dedicated to client privacy and safety. Though one might ask, are these rights in part due to HIPPA, or are they due to the magnanimity of Intermountain Healthcare, after my discussion with Lee, I would wager that both play a part in these decisions, but also that Intermountain does strive to live their mission to help people live the healthiest lives possible.

Since my interview with Lee, I have had more questions come up that I intend to follow up with him. Questions such as how much freedom does a patient have as to what data is collected about them- what data do they have to provide, etc.? If a patient prefers to minimize the amount of data collected and stored about them, does that preclude or limit their ability to receive care from Intermountain? How much of that data is shared with the National Health Record databases and can a person limit the amount that their data that is shared with the database? I hope to re-connect with him soon to answer these questions, to continue the research into Intermountain's vast administering community and how they keep track of all the information that they have at their fingertips.

BIBLIOGRAPHY:

https://intermountainhealthcare.org/

http://www.differencebetween.com/difference-between-filesystem-and-vs-database/