**Project Nightingale**

**What is Project Nightingale:**

(Wilson, 2016)

Having searched Project Nightingale online, I found the projects official website, it is a pre-commercial procurement meaning it is not yet fully commercial on any market, the end goal is to design a wireless wearable device that can into a medical practitioners clinical decision on the well being of a patient.

The project is currently nearing the end of phase 2 and the prototype is already seeing live use in selected hospitals.

This device will continually monitor a patients vital signs, this includes blood results, heartbeat, blood pressure and other necessary clinical data, with 24/7 monitoring the goal is to give patients and practitioners an early warning of health deterioration be it in or out of the hospital.

From reading this alone and ignoring what I know of the project, I have to say its an idea I can get behind, 24/7 monitoring to me initially seemed a bit much and intrusive, but being able to detect health issues that may not be immediately noticeable to a human could save countless lives, people who have terminal illnesses that could have been avoided with earlier detection would welcome this device in a heartbeat. The issue that will come up here and it’s a question for every individual who values both their health and privacy is which of the two do you value more.

Now to find out where I stand with the research I will conduct.

**The Guardians Whistleblower**

(Pilkington, 2019)

My introduction to this project was through an article the Guardian Newpaper wrote up, they were contacted by whistleblower who informed them on a secret transfer of up to 50 million Americans personal medical data, from on of the largest healthcare providers in the US to Google, the accused healthcare organisation is called Ascension. It was reported that the data was being transferred with full personal details including name, address, date of birth and medical history, this data was not anonymised through a process known as de-identification and was fully accessible by Google staff in its entirety.

There’s no doubt that device being built will need countless samples of medical data to draw up conclusions on a patients health, but these devices should not need any individuals personal information, to me the real question is what does Google want with this personal data or maybe Ascension made a catastrophic error and didn’t intend on transferring the personal elements of the data. This is speculation as I research, clear answers may surface as I dig deeper into this issue.

Another major issue that sticks out to me is that all this data is being transferred with the knowledge or consent of both patient and doctor.

One of the most outstanding problems to me came on the second page of this write up when it was noted that an employee and I quote “expressed concerns of individuals downloading patient data – need to make sure everyone is trained to not be able to do that”. I find it disturbing that professionals in my field of study where recorded making such a quote while I, a mere college student, know that people should not have to be trained not to this because it should not be available action to perform in the first place.

Not just in the case of this incident but in general I firmly believe that we all should have easy access to information on how our data, personal or otherwise, is being controlled, managed, stored and used, whether it be in the pursuit of improved medical care, advertising or in any other aspect. Despite Google and Ascensions claims to compliancy to HIPAA federal health laws, the patients should be informed about their data being used and should absolutely be given an opt in or opt out option. The fact that this is all being done secretly tells me that they intend to use the data for other means, such as targeting patients using the device with medical advertising, never lose sight of the fact that with these big companies it all comes down money and how much they can make.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

(Office of Civil Rights, 2013) (Rouse, n.d.) (Stryker, 2013)

With both companies claiming that they are being compliant with HIPAA federal health laws, after researching this law I discovered that it was up to medical practices to review their relationships with each of its vendors not currently recognized as a business associates. What I gather from this is that each vendor must meet a required set of rules to become a business associate of a medical practice.

I am assuming that Google has passed this criteria the detailed documents have the rules embedded with in them but finding them has proven to be fruitless. An important rule to note is that:

“business associates are independently responsible to comply with HIPAA privacy rules, Practices are no longer responsible for HIPAA infractions committed by their agent Business associates.”

From this quote, at this time of writing it would seem that Ascension are in the clear with this data breach so long as the data is secure in transit, least from a legal stand point, their reputation will surely take a blow with their name constantly coming up though this negative publicity.

With Google now identified as the sole company to breach these rules and this company being a business associate of Ascension, I moved on to research Business Associates Contracts. Within this is also stated that business associates must follow the HIPAA rules for security and privacy.

Under “Permitted Uses and Disclosures by Business Associate” there are cases where information can be disclosed as a requirement of law.

But business associates must secure the authority to use protected health information, this information then must be de-identified to keep individuals anonymous, Vendors can then specify the manner in which a business associate should de-identify the information if they wish. I would say knowing this that while Ascension remain in the clear, it was irresponsible of them to not request Google to apply a desired de-identification method to all of the medical records.

Following on this business associates can disclose protected health information for management and administration or to carry out legal responsibilities, provided the disclosures are required by law, or the business obtains permission from the individuals on whom the information is being disclosed, assuring that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the individual. The individual can then notify the business associate if they discover that the confidentiality of the information has been breached.

From what I can understand little to none of the above paragraph has been enforced, all these documents have been moved in complete secrecy with a patient or doctors consent, no patient had been directly informed that their medical data has been used in any kind of manner outside of a hospital and for what purpose it serves. The Whistleblower has confirmed that all the information is in its original state and free to access by Google employees, any irresponsible or malicious employee with in Google could very easily put these documents to a public domain.

Here’s where I come to a difficult question, I’ve already stated that little to none of the proper procedures were being followed and while I disagree with training employees not to do something they shouldn’t have the ability to do in the first place, would there be a breach of information here if the Whistleblower didn’t come forward?.

I don’t think this very particular issue on a data breach would be a problem, but the presence of a disgruntled employee proved that you shouldn’t trust a large group of people handling what they can see is highly sensitive and confidential information, we find ourselves going back to the fact that Google should have de-identified the data and being suspicious of what they intend to do with peoples private information.

This issue still remains very shady to me, I can see the good behind the whole project and firmly believe most of the people working on it are doing so with the sole intention of improving medical care, but the corporate giant controlling it all has to me has extra intentions that no doubt revolves around making money, it’s all business at the end of the day.

**Further Research**

(Garrity, 2019)

As this is still an ongoing development I will write all my further findings here that I feel is relevant to this topic and will ultimately end with my concluded opinion.

Since the Whistleblower came forward Ascension have raised concerns about the way Google is collecting patient data, they have gathered lab results, diagnoses and hosptialisation records. I feel that results and diagnoses are necessary for Google to obtain in the development of this project, after all how are the supposed to build technology that can early detect symptoms if they have to previous records to refer to. Hosptialisation records is a bit grey, I right now feel that is not necessary to hold records of this, when and for how long a patient was admitted while it may help to know to some degree, I don’t think it is needed in determining an illness a patient may have.

Ascension have also cited that:

“in some cases Google has access to patients complete medical history.”

There is a lot of room for argument in the amount of access Google should have when it comes to a patients medical history, having details of all symptoms, illnesses and treatments over a patients life time will prove invaluable in the pursuit of perfecting this technology, but many problems come with knowing this, even if all the personal information was de-identified one may be able to determine who a patient is based on unique illnesses, limitations to treatment which could be for religious reasons and for most patients a birth record will be recorded making determining a date of birth a relatively simple task. This is not all that one could look to find a patients identity, an entire medical history will no doubt have seemingly anonymous data within it that can be used to find any patient, even the name of treatments on the record can determine if they ever were hospitalised while abroad.

Form this the real question I am now looking to is how do you completely de-identify a patients record while still retaining all the necessary information? I’m certain that the answer is that you can’t, and I don’t say this in the defence of Google, from my findings it is clear that they have breached HIPAA rules for privacy and security and should have to answer for I, its been said before and I’ll say it again, their employees should not need to be trained to not look at patients personal records, one they should not have access to these records and two the data at the very least should be de-identified.

The fact that all this data will be moved to Googles cloud platform in its current state is highly alarming, there’s no doubt that Google, despite what I’ve learned of project nightingale, has extremely strong security measures, there services are not easy to breach and generally email accounts get owned through users using then to register with other websites, take the infamous Ashley Madison data breach from a few years back which saw a lot of users personal information get exposed. This does not mean that I view Google as 100% reliable if history and the internet has thought us anything is that people will find a way in, even the mighty Blockchain protocol will be breached eventually.

In all this patient should not only worry what Google might secretly do with their data, but what those who breach into the cloud system its stored on could do, the people that will break into this system will likely do so with complete anonymity, neither patient or Google will know of their presence, we do have to consider that the greatest mastermind criminal thieves have never been caught.

This brings me to my final point before my conclusion, what dangers could patients be in with their personal data in the hands of individuals outside of Google who obtained it illegally? While I usually go to the obvious identity theft, which can lead to but not limited insurance fraud and bank fraud, which can bring a lot of trouble to an innocent individual and is a real possibility I don’t to come across as dismissive to this problem, but the real goal is to make money, much like Google. I recently learned that a persons medical data can sell for anywhere between €100 and €200 on the dark web, who these records are auctioned off to would be where the former problem I mentioned will come from. Consider that Google plans to move 50 million patient records to their cloud service with all their personal data included, that can bring the records dark web value up to a minimum of 5 billion Euro, or to use the dark webs favoured currency its 734,450 Bitcoin (BTC) as of writing this.

Before I conclude I would like to note that The Wall Street Journal and Search Health IT were looking for me to sign up and/or pay a fee, I stopped pursuing information on these sites as I am not comfortable handing over any info or paying any fees.

**Conclusion**

Considering everything I’ve learned on this, what I know of Google and the natures of people and their drive to make more money, overall the handling of the data is wrong both morally and legally, if it somehow comes that the law gets twisted to state that they have not breached HIPPAs policy, then the legal system in America needs to be reviewed because it should be completely illegal.

This project has good intentions and I personally do not want to see it get derailed, it could potentially save millions if it sees its full potential, but in order for this to happen Google needs to keep its hands clean, the data should be de-identified to the standards of HIPPA and I do feel that Ascension should have specified this before the transfer of data began even though they weren’t legally obligated to. Google needs to carefully consider its cloud storage platform and make sure it exceeds even their own standards of security, to ensure that outside entities do not gain access to this information.

One I do feel very strongly about is the whole lack of consent from patients and doctors about the use of all this data, everyone should have been informed about their data being used for this project and should have been at the very least granted an opt in opt out option, furthermore people should be allowed to know how exactly their data is being moved around and by who it is being used, if its being used to push advertising, methods to gain money or being sold to business associates. Following this this I do also believe that if people opt in to these things and companies are making money from their data, they should most definitely see a percentage of the takings, this is veering off the topic to general data gathering but they are related.

Finally all immediate personal information should not be viewable by Google at all, I would not like any one in Google to view all of my personal data and know that is was me, they can have my medical record alone and with my consent given through my hospital or doctor but they don’t need to know my name, phone number, date of birth, country of origin etc, only what sickness I had and what treatments I took.

I do have to consider how I would feel if tomorrow I got news that I have a strongly potential terminal illness, so long as I stand a chance of being cured I may not care too much about what data is available to who anymore, as the saying goes:

“Healthy people want many things, sick people only want one thing…”.

## References

Garrity, M. (2019). *10 things to know about Project Nightingale: St. Louis-based Ascension and Google have made headlines over the past few weeks over Project Nightingale,*. [online] Beckershospitalreview.com. Available at: https://www.beckershospitalreview.com/cybersecurity/10-things-to-know-about-project-nightingale.html [Accessed 29 Nov. 2019].

Office of Civil Rights (2013). *Business Associate Contracts*. [online] HHS.gov. Available at: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html [Accessed 29 Nov. 2019].

Pilkington, E. (2019). *Google's secret cache of medical data includes names and full details of millions – whistleblower*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information [Accessed 29 Nov. 2019].

Rouse, M. (n.d.). *What is HIPAA (Health Insurance Portability and Accountability Act) ? - Definition from WhatIs.com*. [online] SearchHealthIT. Available at: https://searchhealthit.techtarget.com/definition/HIPAA [Accessed 29 Nov. 2019].

Stryker, C. (2013). *Two Essentials for HIPAA Omnibus Final Rule Compliance*. [online] Physicians Practice. Available at: https://www.physicianspractice.com/blog/two-essentials-hipaa-omnibus-final-rule-compliance [Accessed 29 Nov. 2019].

Wilson, M. (2016). *What is Nightingale? | Nightingale*. [online] Nightingale-h2020.eu. Available at: https://www.nightingale-h2020.eu/what-is-nightingale [Accessed 29 Nov. 2019].