02239 Data Security - Final Assignment

s042457 Brian Lynnerup Pedersen

December 18, 2013

Contents

1 Disclaimer

This report is based on a field study I did on a nursing home (the Center) in Denmark in December 2013. Due to the sensitivity of the topic, the nursing home as well as the people I have interviewed has requested to remain anonymous. Because of the time limits for this assignment, the numbers of interviews is too few to be an accurate indication of the healthcare system as a whole, but I believe that for a large part, this is somewhat representative of how things operate in the healthcare system as a whole. Mainly because the people I have talked with, that have years of experience in the system, told me that what is documented in this report is similar to what they've experienced in other parts of the healthcare system.
The subject as a whole is huge, and can in no way be fully covered by the limits of this assignment.

2 Introduction

For this assignment I chose to focus on topic A (Health Care).

The world today is becoming more and more digitalized. We want to be able to access data from everywhere in a instance. In Denmark more and more communication with all government branches has to be handled on-line. If you want to renew your passport, apply for a name change, report you bicycle stolen and much, much more is the kind of dealing that has to be handled on-line. Before this began, when a person went to a doctor or hospital or the like, they would have actual files in metal cabinets that would contain all your medical data, in the 80's and 90's a shift began where doctors would have your journals on a pc. Later on, the journals would be added to databases, so that a patients medical data could be read by any doctor in the country. This brave new world of digitalization presents a whole new range of options in terms of making the health care system much more efficient, but how well is the process going?

Today many people are treated in the healthcare system daily, some of these people may be people that holds important places in government or businesses. Finding out if such a person is about to die, or has fallen very ill, could create a devastating effect. When Steve Jobs (co founder of Apple) died there was a lot of speculations as to what would now happen with Apple, his death even made Apple stocks fall by 5%. And a year after his death people were still speculating in the aftermath of his death[1]. And the press is still talking about if Apple has any more to offer in terms of innovation.

When Kate Middleton (Duchess of Cambridge) was emitted to the hospital during her pregnancy a couple of Australian DJs succeeded, by using Social Engineering[2], by posing a members of the royal court to obtain information about the Duchess. The nurse that was the victim of this prank call, later committed suicide[3].

Knowing about peoples' general health, can in certain situations be worth a lot of money. In severe cases it can even be a mean to eliminating a person.

This is what I want to try and look into in this assignment. To do this, I was allowed to go to a nursing home in Denmark and talk with some of

[1] `http://business.time.com/2012/09/25/apple-one-year-after-steve-jobs-death-the-iphone-falters/`

[2] `http://en.wikipedia.org/wiki/Social_engineering_(security)`

[3] `http://www.huffingtonpost.com/2012/12/07/kate-middleton-nurse-found-dead-prank-callers_n_2257231.html`

the people working there, and ask them questions regarding data security. I have also called different government offices in order to find out what the official laws and policies are, and how they transcends from when a law is passed, implemented in the various municipalities in Denmark and to the person having to abide to these laws and policies. How is our data secured, and what measures are taken to prevent data falling into the wrong hands?

2.1 Interviewees

I have interviewed the following people and legal bodies for this assignment:

- Leader 1 (**L1**) - Trained nurse - 20 years of experience.
- Leader 2 (**L2**) - Trained nurse - 14 years of experience.
- Leader 3 (**L3**) - SOSU[4] assistant 10 years of experience,
- SOSU assistant (**S1**) - Less than one year of experience.
- SOSU helper (**S2**) - 30 years of experience.
- IT department of the municipality in question (**ITD**).
- "Datatilsyntes"[5] (**DT**).

All staff I have interviewed at the Center, has known what my purpose was at the Center and was informed that any information they passed on to me regarding questions I would ask them, would be anonymized and had no impact in terms of their job.

[4]Social og Sundhedshjælper - Basic healthcare education in Denmark, comes in two degrees, the assistant (similar to a nurse's aide) and the helper which is a shorter version of the assistant education, and thus has less responsibility.

[5]Government branch in charge of enforcing the laws, in relation to personal data - `http://www.datatilsynet.dk/`

3 Structure

During my interview at the Center I found out that the structure is rather complex and hard to define in set boundaries, as to whom has access to what kind of data (and if they have read / write permissions), but I have made some rough groupings. The Center is divided into four different branches that deal with various treatment areas. For each of these branches there is appointed a leader, so in total the Center has four different top leaders, each managing their own area (**Tier 1**), each area has different groups[6] with residents. In the next tier (**Tier 2**) is the people that are leaders in certain areas and nurses doing regular care taking. In the next tier (**Tier 3**) is the SOSU assistants. Below that tier (**Tier 4**) is the SOSU helpers, and in the final tier (**Tier 5**) is people employed with the maintenance, kitchen, cleaning, volunteers and relatives to the people living at the Center, in short people that should have no access to personal data (other than what relatives are entitled to know, as per consent given by the citizen, more about this later on).
As some of these tiers covers different branches of the Center, I will talk about all of a tier or local of a tier. All means that everyone in that tier have access to the data, although they may not work with the resident directly. Local means that only people working with the resident in some way have access to that data.

These tiers is created in order to try and give a clear image of who has access to what data, and is not something that is implemented within the Center.

L1 belongs to **Tier 1**, **L2 and L3** belongs to **Tier 2**, **S1** belongs to **Tier 3**, **S2** belongs to **Tier 4**.

4 Rules, Laws and Policies

Every person that is employed in the Danish social and health care is required to sign a pledge of confidentiality, that makes them promise that they won't share any sensitive data with anyone outside the health care system, which is documented in the Danish law "Forvaltningsloven" §27[7]. Also in relation with "Persondataloven"[8], which is the law that, in **VERY** short, deals with the handling of personal data, ensures the individual persons

[6] Group being a small collection of apartments, or homes. These have their own SOSU assistants and helpers.

[7] `https://www.retsinformation.dk/Forms/r0710.aspx?id=142955`

[8] `https://www.retsinformation.dk/Forms/r0710.aspx?id=828`

rights to their personal data. To that law is made an extension that more in detail describes how data and electronic devices are to be handled[9] Both links are in Danish. These laws are upheld by **DT**.
Every person that is hired in the public sector is also required to have a clean criminal record.

The municipality is the ones that makes the policies regarding IT and data. Which means that the rules regarding IT can vary from municipality to municipality. It is the responsibility of the municipality to inform their employees of where to find information about their IT policy. It is also up to the municipality to ensure that these policies are up to date and in accordance with the law.

The government is the legal body, that passes the laws that deals with data security. This is upheld by **DT**. They are responsible for both "Persondataloven" and "Forvaltningsloven".

4.1 Citizens Rights

As for all other parts of society, every person living at the Center has certain rights in terms as to what data they want to share and with who. The exception here being that some of the elderly people could suffer from various conditions (such as dementia) that would render them unable to take care of themselves. In these cases a legal guardian is appointed to the person. This would often be a close relative, or in special cases the health care system itself can become the legal guardian of the person (this could occur when the person have no living relatives). If a guardian is appointed, this guardian will make all decisions on that persons behalf. These points are all mentioned in Persondataloven, but some of the points I felt should be noted here. These include:

- To whom personal data is passed onto, this being relatives, friends, staff or other government branch.
- In what extend each of the people mentioned above is entitled to informations.
- To create a "Treatment Will"[10]

[9] `https://www.retsinformation.dk/Forms/R0710.aspx?id=842`

[10] This will concerns what kind of treatment for the terminal ill is allowed, including areas as; Wanting a doctor when ill and at what times, receiving CPR in case of a cardiac arrest - in general all things related to the treatment and care of the patient. This will has to be authorized by a doctor, that has to vouch for that person being unrecoverable and terminal sick.

5 Data Security

5.1 General

When I came to the Center I was told that I were for all intents under the rule of the confidentiality law, in other words, if I gained any sort of personal data while at the center, I was in no way allowed to share this in any way. I was how ever never required to sign anything to that effect. Even though an oral agreement is also binding, I could in theory deny ever having been to the Center.
To begin with I asked how they stored their data. Parts of it is stored in computers, and parts of it is stored in archive. Some of the data stored in the archive include, a journal, medical information, treatment plans, agreement pacts[11] and "citizens evaluations"[12], the Treatment Will. This data is accessible by all on **Tier 1,2** and locally on **Tier 3 and 4**.

At the Center they got three different WLANs, two named admin and one named guest. The two admin networks was locked, and the guest one was open. I had obtained no right to "spy" on their network communications (by using Wireshark or similar software), so I did not check for what kind of network usage was going on. Nor did I check if employees was using the secure connections.

At the Center, data is stored both as paper data as well as electronic data. The electronic data is mainly regarding residents journals. The paper archive is resident journals, agreement contracts and medical informations. These papers are kept in file cabinet.

5.2 Archives

The center is divided into groups, in which a number of residents live. Each group has their own work station, that is situated somewhere in the Center, near the residents. Every work station consists of an archive and a computer.

The archive holds documents like the agreement pact and the journal. This journal also contains data about medical treatment. Only staff on **Tier 1 and 2** and locally on **Tier 3** can alter in the medial information. It is "read only" for staff on **Tier 4**.

How ever, special papers like the Treatment Will, is located at the office of the group leaders(Tier 2). It's content is known to Tiers 1, 2 and locally 3 and 4.

[11] This pacts is made by the resident and the Center, it specifies who is entitled to know what about the resident

[12] This is an assessment of the resident as a whole. Outlines how the resident is doing.

During my interview session with some of the staff, I was told that the archives was not locked, neither was the locker containing the keys to the residents home. Although I was told that they should be locked at all times, this was never the case. Ironically the refrigerator was always locked, as some of the demented residents could forget they had been fed, and take food from the refrigerator. This is a case in which the issues of data security become pretty clear. The focus is not on the data as much as it is on the food, as (so far) no one has stole any data. And for logical reasons, the food is often reported stolen if not locked in a the refrigerator, journals have not (yet) been stolen.

5.3 Electronic Devises

The Center is using computers in their daily work. These computers are all secured with a password. Passwords are be changed every third month (the user is prompted every third month to change password). For the work stations there is one shared computer this is mainly used by **Tier 3 and 4**, though **Tier 2** can use them as well. Some of the staff in **Tier 2** have their own personal computer (this being the case for **L2 and L3**) and everyone on **Tier 1** have their own computer. All users of the computers have a specified access level. This means that the user have varying programs available to them. The Center is using two different systems for residents journals. One containing more data than the other. Both are connected to a database. All work done by the staff have to be saved on remote drives, as their C: drive is reset every night (**ITD**). To access these systems, the users have to log onto a Citrix[13] secure line. The users have an USB drive, that they have to plug into the computer, that grants them an access key to their WLAN.

The Center has also begun using iPads for resident data, how ever there was none in the part of the Center I visited, so I will not go into further detail about this.

All employees are also given a mobile phone, none of these are smart phones, so for this assignment they are of no interest.

5.4 Electronic Data

All resident journals are kept in the databases. These databases can be access by the two programs mentioned earlier. For **Tier 3 and 4** they only have access to one of the two programs, giving them access to data regarding the residents at the Center. Staff at **Tier 1 and 2** also have

[13] `http://www.citrix.com/`

access to a program that will show them information about every resident at every nursing home in this municipality. This program is also used by doctors in this municipality. Therefore it is possible for the residents doctors to write notes in this system regarding medicine and care. However, these programs used by this municipality might not be the same as the ones in the other municipalities, as there is no country wide standard. So there is no possibility to share information with other nursing homes or doctors outside the municipality. This has to be done by the means of phones, mail and e-mail. Hospitals are using an altogether different program and they cannot share information electronically with the Center (or any other nursing home for that matter), so in the case of a resident having to go to the hospital, the hospital will send a paper message along with the resident when they are discharged from the hospital. The staff is also told not to use their email to share personal data, how ever I was told by(**L2 and 3**), that personal data is sometimes shared using Outlook by members of staff. **L1 and L2** also told me that they had a secure internet connection that they should use for internet browsing (protected by Citrix). They never got the information to use this by any official source, one of their colleagues told them so, when the colleague saw that they used the normal internet browser. This was never informed to them by any "official source".

5.5 Paper versus Electronic Data problems

When ever a residents journal is updated, it has to be done both in the paper version and in the electronic version. There is no way to update the paper journal by printing the journal from the computer. If there is mismatching between the two, staff would normally take the electronic version and update the paperv version accordingly to this, after discussing it with the person that last changed in the journal.

5.6 Data Sharing - Staff

The employees at the Center needs to exchange informations about the residents. As the Center has staff working in shifts, this is done to make sure that everyone is up to date with residents health and status. It is possible for everyone in **Tier 1, 2, 3 and 4** to make notes in one of the two programs, containing special information (if the residents are sick, taken to the doctor or similar). This is called "advis". These advis is also how the residents doctors would communicate with the Center.

I was told by **L1 and L2** that the staff on **Tier 3 and 4** only shares

information about resident health by using advis. How ever during my interview with **S1** I was told that information sharing would also occur orally when the next shift would show up for work. **S1** told me that this was mainly information that required extra attention, otherwise it would only be shared using advis. While I was being shown the archives I was also present to two employees sharing personal data about a resident.

5.7 Unintended Data Sharing

The Center has no group rooms in which the staff can discuss the residents health and well being. There's a room for meetings, but that cannot always be access. Therefore a lot of information sharing will happen in hallways, the group kitchens (the Center has one central kitchen unit, and then smaller kitchens locally) and where ever a bit of privacy can be had. The big issue with that is there will eventually be shared information to parties that should not know of this. The maintenance and cleaning staff will also be able to obtain information regarding the residents. This will happen during their daily work routines, that will at some point lead them to be in an area where the other staff can be sharing resident informations. Although the Center strives towards not having information being shared in the proximity of someone that should not be informed, it is hard to achieve this goal with no place to go to. This also leads to relatives being able to overhear information sharing if they are in the hallways when staff is talking about the residents.

The Center also have a number of volunteers. It is a growing problem today, that the elderly have very few or no relations coming to visit. Therefore a group of people have volunteered to come by once in a while and talk with the residents at these homes, and the Center is no exception in that matter. These volunteers can over the course of a persons stay in a nursing home, be able to acquire a lot of personal data.

A lot of the people that are lonely, will often be more suspicious to social engineering, and these volunteers will be hold a lot of information that can be used to manipulate the residents they are visiting. The volunteers are a valuable resource for the Center, helping to give the residents some company. By spending a lot of time they can become a confidant to the resident, and though this might not always be bad, it is an area that could be the target of exploits.

When I was at the Center they were unable to find out if the volunteers was required to sign a pledge of confidentiality, as none of the people I spoke with had anything to do with them in terms of administration. The general consensus amongst interviewees was that they thought the volunteers had

signed a pledge, as the information they would gain from working at the Center, would require that, but no one was able to tell me if they actually had signed such a pledge.

What is a common thing amongst **Tier 5** is that they can have a lot of pieces of information that when put together, can produce a rather complete history of a resident.

5.8 Data Sharing - Relatives

For this section I interviewed two members of staff (**S1 and S2**). For this we talked about "Mr. Mortensen", a fictional resident whom I claimed to have a relation to. My questions is written in **bold**.

If I called this Center, asking about Mr. Mortensen's health, what would you tell me?

S1: "I would not give you any information regarding him. I would tell the resident that you were on the phone."

S2: "I would give no information as in accordance with the law, if you were persistent or claimed to be entitled to that information, I would contact my local leader[14]."

What if Mr. Mortensen is not present (hospitalized or away for some other reason), or is sleeping?

S1: "I would take a message, or if it was urgent and he was sleeping I would wake him and tell him that I was on the phone."

S2: "Same as before."

Is there any exceptions to this?

S1: "I would, if and only if, I knew your phone number and knew you *REALLY* well and Mr. Mortensen has stated in his agreement pact that you are entitled for the information you requested, tell you the information requested."

S2: "No, unless I was 100% sure of who you are, and you were in the agreement pact, but I would talk with my leader first."

If I showed up at this Center, and you hadn't seen me before, what would you do?

S1: "I would approach you, say hi and ask you whom you were looking for."

S2: "I would say hello and ask you if I could help you with anything."

If I said I was Mr. Mortensens grandchild, and asked you about his health, what would you tell me?

[14]This would be a SOSU assistant or trained nurse.

S1: "I would firstly tell Mr. Mortensen that you were here visiting, and then you could ask him if he wanted to see you. But I would not tell you anything."

S2: "I would tell Mr. Mortensen that he had a visitor, but I wouldn't tell you anything."

Are there any exceptions to this?

S1: "Again, if I knew you and you were listed in the agreement pact as entitled to these informations, I would give them to you if Mr. Mortensen wasn't present."

S2: "I would only give you any information if you were in the agreement pact."

5.9 Data Sharing - Outlets

In the large grey area of the this ocean of rules and policies regarding data security we have a lot of people doing their jobs in an area that can be very taxing on the mind. Ranging from the paramedic trying to save people after a car crash, the fireman having to save people out of a burning building to the employee at a nursing home developing a relationship to a resident and then perhaps one day watching that person die.

In order to cope with all the impressions these people get on an every day basis, they need an outlet through which to lighten these impressions.

A lot of this is done at the Center between colleagues. Many will have been involved in the same resident, and when that person dies, they can use their colleagues as an outlet.

But as with any other job, you talk with partner when you go home about your day, and what you have experienced throughout the day. This is by law illegal, but a very human thing. All the people I have interviewed for this assignment all told me that they would talk about their day when they came home. They were careful not to mention names or other personal information that, at first, could give any information as to who the resident they were talking about could be.

However, every little bit of information is a piece of a puzzle, that can in the end unravel the identity of a person. And as with the **Tier 5** this group could obtain a lot of knowledge that they should not have.

5.10 The Rest Is Silence

What happens with our data when we die? At least in the case of the Center a death will be looked at in two different ways, unexpected or expected.

The unexpected is when a resident that is otherwise looking healthy dies, an expected death is when the resident has been poorly for an extended period of time, with health declining.

In the case of an expected death, the residents own doctor is called up, and will then declare the person as deceased. In the case of an unexpected death, this is treated like any emergency case of cardiac arrest. 112 is called and this type of call makes an Paramedic and a doctor to arrive in an ambulance. Because the death is unexpected the police will also be present.

Within 24 hours, all personal data of the person would be erased (at least from the two systems that the Center used). With the exception of CPR, name, date of death and last know address.

5.11 Lost Electronics Devices or Journals

I asked **L1, L2, L3, S1 and S2** what they would do in the case that journal or a computer was missing (and they were 100% sure that is was either stolen or lost without any hope of being found again). All, but **L1** replied that they would go to their nearest leader in both cases. **L1** said that in the case of a missing journal, that would be reported to the police. In the case of a missing computer or iPad, no measures would be taken as they are protected with passwords. They would be reported lost to **ITD** so they could replace the missing piece of gear.

6 Access Control

The home is open during the day time, after which the doors are locked. After the doors are locked, there is a doorbell which can be used to alert the staff who can then let you in. There is no video surveillance at the Center. **L2** also told me that there in general is no sort of access control to health care institutions in Denmark, other than what the staff enforces by approaching people. All offices are normally unlocked, and the workstation of the various groups are also in the "common area". So access to archives or computers does not require any codes or keys, nor are these areas monitored at all times.

L2 also told me about a situation in a hospital where **L2** had worked, where while using the computer (typing in a patient journal) an emergency situation occurred and everyone left the room with the computer in. When **L2** came back, there were evidence of the computer having been used, but **L2** never found out in what way or for what.

7 Enforcing Data Security and IT Policies in the Municipality

After visiting the Center, I called up **ITD** in order to get some answers as to how they handle data security within the municipality. This has to be a big issue, when a lot of the people working for the municipality have access to personal data, being they work as a teacher, a nurse, a SOSU or working a city hall. When I called them I was talking to one of leaders of their **ITD**. She told me that although the municipality's IT policy was created in 2006, it hadn't been updated since 2007, despite the fact that the policy states that it should be revised each year.
The **ITD** is in charge of updating the computers in the municipality, to make sure that they are up to the current standards, for instance are they currently upgrading their computers to use Windows 7 instead of Windows XP, which Microsoft stops supporting by April 2014[15]. This **ITD** was actually in charge of the data security on IT equipment in three different municipalities, and that they therefore had to operate with three different standards. In this municipality, if an employee had a smart phone, the phone would lock itself after being unused for a short period of time. In one of the other municipalities they worked for, they also had a program for sending secure text messages on their phones, this however was not required in this municipality. I was also told that the municipality would have a seminar every third month for new employees, and as a part of that seminar there would be a session with focus on IT security and how to make sure your electronic devices was being used in the right way. This seminar had been running for at least five years. However of the five people I interviewed, three of them had been to this seminar. None of them remembered having a special IT session, but only given a number for which to call in case "something did not work". Also staff hired more than five years ago was not given this course, and when I talked with **S2** about data security, there had never been any form of information passed on to **S2** regarding this. All **S2** knew about how to work with data was from what had been told during work.

8 Datatilsyntes - How Laws Are Enforced

I called up **DT** to ask them about how they make sure that the municipalities' IT policies and rules are in accordance with the law.

[15] `http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx`

DT told me that the law, "Persondataloven", is rather vague in terms of how to actually enforce data security. So there is made an amendment that specifies how the municipalities are supposed to uphold the law[16]. Also § 62 of "Persondataloven" entitles **DT** to visit both institutions and municipalities to look into how the data security is working.

When I talked with the staff at the Center, I found several cases where they didn't know what to do in certain situations in relation to data security - like using the Citirix secure internet connection. In the amendment to "Persondataloven", § 5 and § 6 clearly states that the authority responsible for the data security is required to 1) inform employees about the data security rules and tools that are being used, and 2) update their IT rules and policies at least once per year to make sure it is up to date. This was last updated in 2007.

I wanted to know how often they made use of § 62, how ever I was told that this was a possibility, and there was no schedule after which these visits are conducted. Of course there is a lot of municipalities and a lot of institutions, but judging from what I was told by the staff at the Center, that had worked in other municipalities, this does not appear to be an isolated case.

9 Final Thoughts

Is security being enforced well enough at health care centres in Denmark? Harder to scam companies, is people next? Social engineering.. Access control, social engineering, identity theft in relation to lost electronic equipment.. Problems with not making sure data security is enforced. Problem with tier 5, could potentially know a lot they're not entitled to know.. Different standards from municipality to municipality - makes it hard for Datatilsynet to make sure that everyone is doing enough to be uphold the law?

There is clearly a lack in control from government level down to the person working with personal data - at least from the Centre's point of view. Staff are not being briefed properly, the municipality fails to update their IT rules and policies in keeping with the law. On top of this is the government branch **DT** that also fails in making sure that the rules are upheld.

There is a lot of problems with the way personal data is handled. One of these problems is based in the fact that we are all human beings, and as

[16] https://www.retsinformation.dk/Forms/R0710.aspx?id=842

such make mistakes. At the bottom line of all this we must consider another, and all together much more basic issue, when a person is deemed unable to take care of themselves and custody is appointed to another.

When an authority decides that a person is no longer able to take care of themselves, are we then sure that this is the right decision? To take a person right to decide for themselves away from them, is to take away their most basic rights. If this happens, we need to be 100% sure that it is in the best interest of that person. This could be exploited very easily. As with the Treatment Will, this is an action that needs to be approved by a government body, and hopefully they will be impartial and qualified to make that decision.

10 Conclusion