Medical Records – the Different Data Carriers Used in Sweden from the End of the 19th Century Until Today and Their Impact on Confidentiality, Integrity and Availability

RIKARD FRIBERG VON SYDOW

Medical records have been used during all medical history, since Egyptian medicine almost 2000 years before Christ, and since the famous physician Hippocrates in Ancient Greece (Tweel/Taylor, 2010, p.1, Nilsson, 2007, p. 12). During the 20th century medical records have undergone a tremendous change in appearance. What has changed is not really the type of information in the medical records themselves, but rather the quantity and the quality of information, the type of data carrier that has been used, and how access to the records has been managed. Medical records have gone through many different phases, from the notebook of the individual physician, during the late 19th and early 20th century, when medical files were rare and only appeared in larger hospitals, to the period of the medical paper file, peaking from the 1950s until the 1990s. During this period, medical records grew thicker in a changing and more information dense health care, as more professions than physicians wrote down how they treated the patients, and as more tests were done on every patient. In the 1990s the most recent change started, as the file changed from being in paper form, using paper as data carrier, to being in digital form using different server solutions to store patient information. During the 20th century medical files grew from being around one page in the beginning of the century, four to five pages in the 1950s, and what can be described as a larger pile of paper towards the end of the century (Nilsson 2007, p. 143). This indicates a fast growth of information regarding patients during this century. Today several sources create the medical records: information from the patients themselves, information from different examinations, observations, tests and sampling. The source of information can also be persons related in some way to the patient, such as a child, a parent or a spouse (Sandén 2012, p. 16).

I am interested in how the changes that medical records have gone through have affected the confidentiality of the records, the integrity of the information they contain, and the availability of the records (for both patients and others). This is what will be investigated below.

Today well managed medical records that contain information regarding a patient's care, are regarded as a precondition for a good and safe care of a patient (Sandén 2012, p. 15). The concept I will use to analyze the changes over time regarding medical records is the CIA Triad, which is commonly used in the contemporary information security discourse. To use a method of analysis from contemporary information security on a partly historical material, might be unusual. I believe though, that there are gains in doing so. We will have a possibility to find problems related to information security that have affected information now in the archives. This, in turn can give us a clue as to how reliable these archival sources are to researchers today. By comparing different periods, we will also gain insights into what might influence and motivate contemporary information security. How will this be done? My investigation will be presented in the form of an essay. First I will explain some important terms from the discipline of information security that will be used in the analysis. Second, I will use these terms on medical information during three different time periods that I define below. The focus will be on the administrative routines regarding medical records in Sweden. Towards the end of the essay I will discuss the differences between the different time periods as well as the kind of problems we might face with medical information in the future.

There is to my knowledge, no other research that uses information security methods as a means of analyzing medical information and compare different time periods and ways of handling medical information. There is of course other research on medical records. I have used Inga Nilsson's doctoral thesis from Lund University 2007 "Medicinsk dokumentation genom tiderna – En studie av den svenska patientjournalens utveckling under 1700-talet, 1800-talet och 1900-talet" to gain historical insight regarding the development of medical records in Sweden. Parts of the discussion I am interested in have been presented in Ulrika Sandéns doctoral thesis from Umeå University 2012 "Sekretess och tystnadsplikt inom offentlig och privat hälso- och sjukvård – ett skydd för patientens personliga integritet" (Sandén 2012). Sandén discusses, among many other issues regarding medical records, how the recent changes in technology have changed the discourse of secrecy and confidentiality, using e-mail, text

messages and social media as examples (Sandén 2012, p. 43). Both these dissertations are used as sources and background material in this essay.

Confidentiality and other important terms

Medical records consist of information. Information regarding a patient's health. This will be the case in any period of time – from the antiquity to our time. It could not be in any other way at least as we understand medical records (and information) today. This makes it possible for us to use the terminology of information security to investigate the changes that have occurred in the use of medical records during the 20th century. In contemporary information security, the CIA Triad is one of the concepts used to describe aspects of information connected to security. CIA (sometimes in the order CAI to distinguish it from the US intelligence agency) is an acronym for confidentiality, integrity and availability (Andress 2015, p. 6).

Confidentiality refers to our ability to protect data and information from persons who are not allowed (or authorized if we are working in a formal organization) to view it (Andress 2016, p 6). In our contemporary digital world confidentiality is kept in organization by password protected systems, encrypted e-mails and by access control systems that keep the non-authorized away. Earlier in history similar systems were used, though being analog. Analog encryption, safes and vaults were common examples of such analog systems. However, the systems should not be considered the most important aspect in keeping the confidentiality; it is really the persons working inside an organization that constitute the soft spot of every security system.

Close to confidentiality is another term, privacy. Privacy has been defined in many different ways over time and is really hard to define in a convincing way. Raymond Wacks who has written multiple works on the subject has described an acceptable definition of privacy as "frustratingly elusive" (Wacks 2015, p. 42). I will sometimes also use another term, personal information. In the discourse of health records, this term situates itself closer to the patient than to the security system or to the ethics of the medical staff. Personal information – information connected to a person – might be private but with different degrees of privacy depending on what kind of information in the health record that we are referring to. Personal information could be described in a two axis system in which "desire to control" and "quality" are the two factors used to describe it. Desire to control is connected to ourselves as persons, to how we value a piece of per-

sonal information. Quality is how dense and exact the information is (Wacks 2015, p. 46). In the context of medical records, we can use two examples. If I broke my leg skiing last year there will be a large amount of (personal) information regarding this in my medical records. The information might be very dense and exact, thus of high quality. But my desire to control it might be small – how embarrassing is a broken leg? But maybe I was treated for a sexually transmitted disease last year. The information in my medical record regarding this might be very brief. The result of a urine test and a prescription of antibiotics. Not dense, not exact, but there might be a high desire to control it from my position. Personal information is a valuable tool of analysis – it regards both a normative function (desire to control) and a descriptive function (quality) as axis in the evaluation (Wacks 2015, p. 46).

There is also another term we need to be acquainted with that relates to confidentiality. In this text I will use the term "leak" (of personal/private/confidential information) to refer to a breach of confidentiality. A leak can happen in any information system that tries to introduce confidentiality and it will happen in any information system without confidentiality. Leaked information has, depending on motivation and resources, a possibility to spread. These possibilities have varied over time, as will be described later in this text. Confidentiality can, in short, be defined as the protection against unauthorized access to information and the protection against leaks of information.

Integrity is the next term in the CIA Triad. In information security, this relates to the possibility to hinder and monitor changes in information and data (Andress 2015, p. 6). If changes are made we need to know who did them and when. An information system that values integrity will produce documentation of how and when changes of the information have been made. We also need protection connected to our information so that only people who are authorized have the possibility to do these changes. The security measures needed to keep the integrity are close to those mentioned above regarding confidentiality.

Availability is the last part of the CIA Triad. Data and information are available when we can reach them (Andress 2015, p. 7) and the availability of the information is measured by how reachable it is. In a digital environment, the availability can be depending on the up-time of our servers, or the quality of our data connections. But also the rules of secrecy connected to confidentiality may have an impact on availability. In an analog environment, however, rules of secrecy and administrative opening hours, among

other things, regulate availability. In connection to confidentiality, availability can be seen as the possibility for an authorized person to reach the information. If medical records are available to more persons than those authorized persons there is a breach of confidentiality.

Medical records from the end of the 19th century to today

This essay will focus on a time-frame that begins towards the end of the 19th century, around 1880, and ends in our contemporary period in the 21th century. I will also do some observations of what we could be facing in the future, based on what is happening today. The time-frame will be divided into three different parts, connected to differences in records management and in the medical professions. These differences are partly connected to the data carrier that was in use. Data carrier, or data media which is another term often used, is a medium that can hold data or information. Examples are papers or hard drives. I use data carrier in a slightly wider sense, also including parts of what we could call the information system – the paper file, the notebook or the digital file. The three different periods of time I will use are overlapping and not in any way absolute. I will try to make an illustration of what can be considered a normal administrative procedure during each period. The first period is called "the notebook and the proto-file" and starts at the end of the 19th century. During this period, the information connected to the medical care of patients was scarce, but a change started to happen in larger hospitals. Two data carriers dominated information management in the medical profession, the portable notebook in which the professional could write notes about their patients, and the early paper file, which I call a proto-file. The proto-file is more connected to a hospital environment than the notebook and consists of different forms about the patient that eventually would make up a file. The next period starts after the Second World War and is called "the filing cabinet". During this period, which lasts until the 1990s information in medical care grows. Systems are created to manage information and laws are written to secure it. The main data carrier during this time is the paper file. The third period starts in the 1990s and continues until our days. I will call this period "the digital file" after its main data carrier – digital files of various types connected through an information system. Digitalization of medical information started as early as in the 1950s but it was not until the 1990s the whole medical record became digitalized, not only statistics and separated data. With this overview, it is now time to turn

to the results of the first period dominated by the notebook and the proto-file.

The notebook and the proto-file 1880–1950

Outside the hospital environment, we can only speculate how information about patients and their medical conditions was treated. Of course, physicians and other health professionals outside of the hospitals took notes about their patients. These are sometimes preserved in archival institutions. One example is the midwife diaries (*Barnmorskedagböckerna*) in which midwives took notes regarding births they were involved in. A database search in the National Archival Database of Sweden shows that the earliest midwife diaries that have been preserved originate from the end of the 19th century and the latest from around 1950. They are very few in numbers, reminding us that the only documents kept in the archives are records that have been delivered to the archives in the first place. We simply don't know what happened to those diaries that were not delivered to the archives. They might have been destroyed or maybe they were kept in private possession.

We have a better grasp of those medical records that were created and kept in a hospital environment. These records were regulated in the hospital instructions. The earliest instructions preserved which mentions medical records is from the Royal Seraphime Hospital in Stockholm and dates from 1851. This instruction only mentions that the responsible physician should write the journal of his patients, and that the head physician should sign it when the patient was dispatched or deceased (Nilsson 2007, p. 73). In 1863, The Royal Health Commission (Kungliga Sundhetskollegiet) published directions regarding what information that should be included in each patient's journal. Some of these were obvious from a patient's perspective (name, disease et cetera) and some of them maybe less obvious (profession, paid fee et cetera). They were to be used by all larger hospitals in the country and were presented together in a printed form (Nilsson 2007, p. 75).

During this period two kinds of data carriers were in use: the notebook and what I call a proto-file. As mentioned earlier, I use the term proto-files for forms that could make up a file when stored together. Sometimes, we may guess, files were created by putting together different forms connected to the care of the same patients. At least the opportunities to do so were present. The task now is to analyze these two different data carriers by applying the different concepts of the CIA Triad.

Regarding confidentiality, what kind of unauthorized access or information leak could occur within the premises during this period? Two kinds of data carriers exist during this period, both consist of paper, and the information is handwritten to the surface. The data carriers are used in slightly different circumstances. The notebooks, the midwife diaries being one example, were carried from patient to patient. There is a possibility that they could be lost during the way, dropped, forgotten in a patient's home, or stolen in some way. If this happened they could be read by those who found them. The only possibility to copy the information during the period, copying being a prerequisite for a leak to occur, would be by hand. This is a process that takes a lot of time and effort from the person doing it. From a physical point of view the proto-file is a little safer as it is kept in a hospital and not moved around the way notebooks are. There is a possibility that they were kept under lock and key when not in use. If this was the case, the possibility of confidentiality rises. Regarding the possibility to copy the information, the situation is similar to that of the notebook.

As for integrity – the possibility to know if any information stored in the data carrier has been compromised or changed – the situation is quite similar for the proto-file and the notebook. They are both written by hand, which makes the possibilities to change the information low. The notebook was somewhat of a personal item, and, so, was usually written by one hand only. The proto-file could be written by more than one person, making the possibility of unauthorized changes a little more likely. Of course, there could be forgeries of the handwriting used, but this calls for quite a lot of effort from the perpetrator's perspective.

As for availability of the information to the medical staff, both these data carriers are location-bound. The information stored in them can only be available at one location at any given time. If the notebook or the proto-file is lost, all information regarding the patient is lost too. From the patient's perspective, the availability of the information is low. There is no evidence that patients had access to their own medical records. But, during this period, the density, the amount, of information kept in medical records was very low compared to today. Information could thus have been transferred through conversation among the medical staff.

The filing cabinet (1950–1990)

The next period starts somewhere between the year 1900 and 1950. The change happened gradually so we will use 1950 as the definitive year when the period has begun. The period 1900–1950 is within the time-frame

during which the modern concept of record management is introduced in Sweden and when standardizations of forms and paper-size are introduced (Järpvall 2016, p. 68ff). The archival concept of provenance – that records created by an organization should be kept together as one archival unit – is introduced in Sweden by *Riksarkivet* (the National Archives) in 1903. At the same time the first common records inventory-system, the *allmänna arkivschemat* ("the common archive inventory") is introduced (Smedberg 2012, p. 246f). This is the period of time when order and accountability are introduced in a wider perspective in record management in Sweden. This is also when office work is standardized and organized in an effective way, making it possible to transfer information effectively. This development peaks in the 1950s when the punch card machine becomes so standardized that it could be used in ordinary office work. A number of other machines and standardizations during this time made administration more effective than ever. According to media historian Charlie Järpvall, who has investigated the effectiveness of the paper medium in 20th century Sweden, these changes had a major impact on the possibility of transferring information using paper as a data carrier (Järpvall 2016, p. 108). Information could therefore be transferred in a much more effective way than before through photocopying or using typewriters. This will have a major impact on how we will view the medical records when we analyze them using the CIA Triad later on.

Towards the end of the period, in 1985, the use of medical records is standardized in a more regulated way through the *Patientjournallagen* (1985:562), the new Swedish law regarding medical records. *Patientjournallagen* was introduced after a long inquiry in which older routines and regulations already in use in Swedish hospitals were investigated and evaluated. The integrity of the patient was the focus of this evaluation. I will use the inquiry that was made prior to the law, SOU 1984:73 "Patientjournalen – Huvudbetänkande av journalutredningen", as my main source of information about regulations and routines and I also use its description of the historical development as a background.

After the Second World War two changes occurred regarding medical records that had a major impact regarding the use of the records. First, in 1947, Sweden introduced the personal identity number, a unique identification number for every citizen. The number consisted of six digits stating the date of birth (YY-MM-DD) and three digits connected to the person's birthplace. The last of the three birthplace-connected digits was even for female persons and uneven for male persons. In 1967 an extra digit, a

checksum that could be derived from the rest of the personal identity number, was added whereas the connection to birthplace was removed in 1990 and replaced by a random number (SCB 2016, p. 4ff). Medical records were soon sorted using the patients' personal identity numbers, thus removing the problem of sorting records when more than one patient had the same or similar names (Nilsson 2007, p. 147). The second important change is that medical professionals stopped writing medical records by hand. Instead the typewriter was used, which, in general, made the text in the records easier to understand (Nilsson 2007, p. 147).

Medical information increased during this period (Nilsson 2007, p. 143). The proto-file had become a file, and the file was increasingly thicker. According to Cornelia Vismann a file is "a repository of authoritarian and administrative acts" (Vismann 2008, p. xiii). These files, being an amalgam of decisions, data and information regarding a patient materialized in the form of a collection of paper bound together by a cover, one file for each patient. Medical care had become more and more advanced and dense in information. The staff was larger, with more experts involved contributing with their piece to the information puzzle of the medical records. From the beginning only physicians documented their information regarding the patients. During the 1950s and 1960s physical therapists and nurses were among the new professions that contributed information to the medical records. Before, the physicians wrote all documentation themselves. Now there were secretaries employed at the hospitals taking notes and transcribing recorded investigations of patients (SOU 1984:73, p. 65ff). The typewriter had a key role in this work. It was the main production instrument creating the records. But several other technical achievements connected to information were introduced in the medical sphere, alongside the typewriter. Early computer registers were used, although complete medical records in digital form were not used until the end of this period (SOU 1984:73, p. 146f). The photocopier was invented as early as the 1930s but was not introduced on the market until the 1950s (Encyclopedia Britannica: Photocopier). It could be used to make copies when records were needed in more than one place at the same time. It also made it practically possible to give the patient a copy of his or her medical records which the new Patientjournallag stated should be done upon request (Patientjournallag 1985:562, § 16). In 1980, something crucial regarding patients' rights was introduced. If approved by the *Socialstyrelsen* (The National Board of Health and Welfare), patients could have their medical records destroyed (SOU 1984:73, p. 15). When the inquiry was released in 1984, 331 patients had

applied to have their medical records destroyed. Only 164 decisions had been made due to low work-capacity. Fifty percent of these were connected to psychiatric care. In most cases destruction was granted. In 66 cases Socialstyrelsen decided not to destroy the records, and in 18 cases the records were partly destroyed (SOU 1984:73, p. 180).

If we apply the tool of analysis, the CIA Triad, what can we say regarding aspects of confidentiality during this period? There are some differences compared to the period described earlier. Firstly, there are more professionals taking part in the care of the patients, the effect being that more persons have access to the medical records. They would all have to follow the same rules of confidentiality, but the risk that information could leak without a possibility to trace information leakage, is indeed larger. The files not used would, hopefully, be under lock and key, in a safe archive space, the only persons that could reach them being those having the key. There are no possibilities to check if anyone has accessed the information. Even if mandatory signing of medical records could be a way of tracing who has been reading which record, there is no way of determining if the signatures reflect who has actually read the record. Secondly, the photocopier gives us both a possibility to copy the medical record (to access it or to give access to unauthorized persons) and a possibility to spread the information, thus creating an information leak. If we want to access our own records, there will be measures to increase confidentiality. There will be a clerk or other types of authorized personnel between us and the record, and if the system is working they will check our identity before giving us access. This procedure will be different in the next period that we will examine.

There are some problems connected to integrity during this era that we need to discuss. The technology both adds the possibility to control the integrity and to compromise it. The personal number increased integrity by adding proof that a file was connected to a single individual. This could have been a problem earlier, when only names were used to identify a person and sorting was done using the last name. Personal numbers could now be used as an authenticity method improving both the control and the sorting of records (Nilsson 2007, p. 119, p. 133). But some of the other technologies could compromise the integrity. The photocopier, mentioned above as a possible confidentiality breach, could create multiple copies creating the problem of deciding which version of a file was used last. Before, handwriting was mentioned as a possible proof of integrity, creating the possibility of checking if the same person had done multiple entries. The typewriter changed this, making it hard to decide who had made different

entries, especially over a longer time. In a serious situation, there would have been a possibility to investigate at least which typewriter that had been used. This had been done in a famous case from 1952, when slanderous letters were spread to compromise candidates in a bishop-election to the diocese of Strängnäs. When a suspect (one of the candidates) was found, the typewriters in his workplace were analyzed, checking the types for differences that would match the text in the letters. Proofs were found, and the suspect was later convicted (Brottets Krönika 1954, p. 579ff). But, without possibility to a thorough examination and analysis, handwriting is a much easier way to prove integrity.

Regarding availability there were possibilities for patients to access their medical records before the new law in 1985 if they applied at the hospital (SOU 1984:73, p. 57ff). They also had the possibility to have their records destroyed, thus making availability impossible for both patients and staff (SOU 1984:73, p. 179ff). A problem with destruction of records is that it cannot be made undone. There is always a possibility that the patient regrets the destruction afterwards, especially if any mistreatment done during one period of time could be grounds for financial compensation later. The medical staff had less control of availability of the medical records during this period, compared to the earlier one. The increased number of staff using medical records made the disappearance of records a threat. According to the inquiry made before the new medical records law of 1985 up to 20% of the medical records could not be found when the staff needed to use them. This was recognized as a problem that compromised patient safety (SOU 1984: 73, p. 145).

The digital file (1990–)

Today medical records have gone through a radical digitalization, just like many other types of records. This process gained speed during the 1990s and the borders are somewhat fuzzy between the period I call "The filing cabinet", and this later period. The digitalization was foreseen in the inquiry that led to the medical records law of 1985, mentioned earlier. In 2008 a new law, Patientdatalag (2008:355) was introduced, making the changes obvious in the title, as the word "record" (journal) from the previous law was replaced by "data". Today the main medium used to keep medical records is larger digital information systems (Sandén 2012, p. 75).

The digitalization of medical records gives the medical personnel some obvious advantages. It is possible to reach the record, stored on a server, from terminals in multiple places through a terminal/server system. With

the increase of bandwidth, it might be reachable from any place, in the world, if the system is connected to the Internet. This makes it possible for many different parts of the health care system to use the same original, digital, record, accessing it on a server from more than one terminal. No copies need to be made. In the legal process leading up to the *Patientdatalag* (2008:355), the idea was actually mentioned that the patients could be the owner of, and was to grant the caregivers access to, their own medical record. In the end, this suggestion was not included in the law (Prop. 2007/08:126, p. 78). Instead a protection against the spread of information between different caregivers was implemented called "sammanhållen journalföring" (integrated medical record). If a patient wants his or her medical record protected from being shared to other caregivers this should be granted (Sandén 2012, p. 193).

Unauthorized data access is one of the problems occurring in this period. It can be divided into two types of unauthorized data access, external unauthorized data access and internal unauthorized data access. This is a distinction usually made by computer security specialists, normally for the two different ways a computer system can be attacked. The attack is external if the perpetrator has no privileges in the system from the beginning. In an internal attack the perpetrator has such privileges most likely in the form of a login and a password (Beta Telelink 2017). In SOU 1984:73 external unauthorized data access was not mentioned at all as the computer systems were not being tied to any kind of public network at this time. Internal unauthorized data access was mentioned however and the solution suggested to remedy the problem was education for the staff regarding the information that could be accessed (SOU 1984:73, p. 78). Since the beginning of this period internal unauthorized data access in connection to medical care has been fairly common. This is connected to the fact that medical staff has authorized access to medical records system whereas the only records that they are actually allowed to access are those belonging to patients that they are involved in the medical care of (Sandén 2012, p. 99). In a case from 2016, a nurse accessed her former partner's medical records from her workplace while he was suffering the consequences of an accident. She claimed that she had his permission and he claimed that he had never given it to her. The court's verdict was that she was guilty of unauthorized data access, and that this was regardless of any given permission. Access to the system was given to her as an employee, and as such she had no relation to the care of her former partner. Accessing the records would therefore be illegal regardless of any permission from the patient (Luleå TR 1868-16).

One verdict from late 2016 stands out a bit, both because of the number of medical records accessed and because the case could be described as "semi-internal" unauthorized data access. The verdict is from a case in which a physician had gained access to a large amount of digital medical records from a Swedish hospital. He accessed these records after his employment at the hospital had ended, and after he had moved to a location outside of Sweden. Keeping his login account (and also hacking a couple of other employees' accounts) he gained access to both former patients' and former colleagues' medical records. During the trial the physician claimed that he needed the records for his research (Stockholms TR 4093-15). Unauthorized data access is regulated both in the Patientdatalagen and in chapter four, paragraph 9c of *Brottsbalken* (The Swedish Penal Code) thus making it a crime that you actually can be punished for (Brottsbalken 1962:700). In the end, the physician was sentenced to probation and he also had to pay compensation to the patients affected by his unauthorized access.

A recent change connects the digitalization with the legal possibilities for a patient to access his/her own medical records. Today, this can be done in most *Landsting* (the Swedish main local caregivers) through the Internet with an electronic identification. This kind of access has been debated both in the press and by the lawmakers. This is because there is a slippery slope between the use of this service by the elderly on the one hand, and on the other, the access to the records that might be given to their younger relatives (sons and daughters et cetera) who help them accessing their medical records online. I call this a slippery slope because for some of the elders, the help from more digitally able younger relatives might be the only way to get access to their medical records when these are digitalized. The question discussed is whether the relatives are supposed to have the possibility to view their elder relatives' medical records, a dispute that has not yet been settled legally. Writing this, the matter will be settled in *Högsta Förvaltningsdomstolen* (The Swedish Supreme Administrative Court) during 2017 (Andersson, 2016). Even though there is an upcoming settlement in the case, the problem is not entirely solved. The access to the medical records is regulated by an electronic identification, a file on your computer and a code, or through an application on your smartphone and a code. It might be relatively easy for a relative, or anyone with connections to the patient, to gain access to code + file/application, depending on the patient's personal experience of, and attitude towards, digital security. To the very least it is more likely than before that someone else will gain access

to your medical records. As long as the paper file was used you had to show up at the hospital and present yourself to a clerk, proving in person that you were actually you. These meetings in person are now replaced by an application and a code.

Now we will turn to the analysis using the CIA Triad. Some changes in confidentiality are connected to the digitalization. The possibility of both internal and external unauthorized data access must be seen as an increase regarding the problems of confidentiality. This, in turn, can be a problem for the patient's privacy. Contrary to earlier periods, there might also be a problem regarding the confidentiality of information in general. The possibility to process and store (and leak) large amounts of information is much more substantial today than during the period of the paper file. A leak of information that you would need a truck to accomplish when the information was stored on paper, can happen very easily today as the information can be stored on a USB flash drive that fits in your hand. You don't even need to show up to gain access. This is also the case regarding access to individual patient's files through the Internet and electronic identification mentioned earlier. It seems as though the loss of a human connection (the clerk) might cause a loss of confidentiality.

As for integrity, there might be some issues with the early digitalization. The personal identification number can be used as a natural key in a database. A natural key is a point of reference that can be the connecting item in a database, at the same time as it is readable and understandable to humans (C2, 2017). This can be seen as a positive aspect of the digitalization process because traceability increases when markers of identification (like a personal identification number) can be used both outside and inside the digital information system. But at the same time there are problems with digitalization and integrity. This is linked to the fact that changing data through unauthorized or authorized access has become much easier than when paper files were used. And the amount of data preserved can make it very hard to track all changes that have been made. Another, although less common, problem with the design of the Swedish personal identification number is linked to the fact that a person might have the same number as another if the first owner dies (and the number is reused), or if the first owner lives to be over one hundred years old. This is a factor that the system designer must consider when using Swedish personal identification numbers, which are given to people both at birth and when they migrate to Sweden and are granted citizenship. This needs to be considered especially

if a number is to be used in the information system after the owner dies (Ludvigsson et al 2009, p 5).

As for availability, this aspect of the CIA Triad certainly has increased. The possibility to reach your own medical records over the Internet from your home is something very different in comparison to getting a copy of your paper file. The online record is dynamic – you can see the changes soon after they have been done. The staff also gains availability as the file is reachable from all locations with a computer connected to the hospital network. This is, of course, if the system does not crash. Several times digitalized medical records systems have crashed with great consequences for the work of the medical personnel. During the fall of 2016, COSMIC, the medical records system of one of Sweden's largest hospitals, Akademiska Sjukhuset in Uppsala, crashed. During more than a week operations were canceled, visits postponed and queues rising. The staff had to use paper and pen, which was enough to provide care, but very problematic when all health care processes presupposes support from a digital system (Nilsson, 2016).

Conclusions and problems of the future

We will now revisit the different periods to try and trace what kind of differences, regarding the components of the CIA Triad that have been discovered. After this summary of the main results I will discuss some problems connected to medical records that we might see more of in the future. All of these problems are connected to the digital era that we live in today.

What kind of changes in the confidentiality of medical records have occurred during the investigated period of time? We started in an era where the only people with general access to the medical records was the medical staff. Patients on the other hand had little or no access. The amount of information regarding a patient's care was much lower during this period compared to today. In general, the first period must be seen as providing a higher level of confidentiality than the second and the last. The only flaw in confidentiality was if the records were lost. From the introduction of office machines such as typewriters and photocopiers in the period of the filing cabinet, the possibilities of a leak increased rapidly and reached its highest level in the last period, the digital file. Summing up we must say that the automation has had some drawbacks if we consider the possibilities for information to remain confidential.

Regarding integrity, i.e. the ability to check if information has been changed, we have a similar development as with confidentiality. The earliest system I described was characterized by a high level of integrity. Written by hand the documents are unique in design and hard to forge. As soon as the different office machines are introduced this changes, however. The amount of information increases, and forgeries and other problems related to duplicability are harder to detect. We can argue that integrity increases when the personal number is introduced – at least it hinders some integrity flaws that can appear through errors like sorting records the wrong way or mixing different patients' records. In the digital era, the integrity of medical records is increased by the possibilities to use checksums and log files to spot if the information has been changed. However, the amount of information is huge and if the system is flawed in some way problems of integrity might be very hard to trace.

Availability is the only concept of the CIA Triad that actually increases unproblematically during the period I have examined. "Unproblematically" if we believe that the possibility to access medical information fast is never a problem. From being available to the medical staff only, the medical records can nowadays be reached from your home through the Internet. It is also much easier for the medical staff to reach it, giving them the possibility to read the same record at the same time, though not being in the same place. This is of course only true if the computer system works – the main distortion to availability today is linked to problems with up-time. Digital files that are not possible to use due to an information system not working properly is a serious problem in contemporary clinical medicine, and might make certain medical care impossible.

But is the information regarding our medical care more or less private today than during earlier periods? That actually depends on more factors than the medical records. One of these factors is connected to how (and to whom) we speak about our own, or about our relatives', medical difficulties. Similarly, if we are in a medical profession, it depends on how we speak about our patients' medical difficulties. One discussion connected to this, and mentioned earlier, is the distinctions between confidentiality, privacy and personal information. Regarding medical records the term personal information is most useful. How we, ourselves, treat our personal information is up to us personally to decide about. We can consider the information to be private or not. If we want to release it, in speech or in text, it is our own decision. The possibility to release our own personal information is not connected to any specific period of time or to any specific data carrier. The

important factor is that if a release takes place it is our own decision. However, possibilities to spread personal information will be larger in the period of the digital file, because of the powers of our contemporary information networks.

There are at least three interesting phenomena that are new to the subject of digital medical records, and that we don't know the full extent of yet. These phenomena have been discussed to some extent in the debate regarding medical records, and they are all connected to confidentiality. The first phenomenon relates to data that the patient themselves collect through a Fitness Tracker, a bracelet that monitor your movement, your heart rate and other pieces of information connected to your body. Fitness Trackers could be connected to your medical records in the future. The Trackers have mostly been discussed in connection to insurance, as they contain the type of information any company that provide health insurance could be interested in (SOU 2016:41, p. 402). Several interesting factors could be analyzed through the CIA Triad here, if the information from Fitness Trackers was connected to medical records. One such factor deals with the extent to which the patient is aware of what he or she is adding to the record while using a connected tracker, with the level of privacy of the information, as well as with the period of time the data will be preserved in the digital records system. There are also integrity issues connected to giving access to the records system to different Trackers. This is more of a computer security issue than an actual information security issue, however, and the problems are more of a technical kind.

Another phenomenon that is discussed among medical professionals is "Patient Targeted Googling", PTG (Baker, 2014). PTG is an expression used for medical professionals using the Internet to read and gather information about a patient. This information gathering could be made for a number of reasons, just curiosity being one possible cause. It must be seen as an intrusion of the privacy of the patient, but is difficult to regulate. The phenomenon therefore constitutes an interesting grey area of professional ethics. In the future, problems related to the Internet as an "extra layer of information" connecting different sources, might grow in number and include more professions than those in the medical field.

The final phenomenon discussed here that might give us a headache in the future is a possible increase in external unauthorized data access. This could happen when more and more repositories of medical records are connected to the Internet, and it has happened, for sure more often than we know about. In 2016, there were reports of over 10 million hospital records

being for sale through the anonymous Darknet-network. The records supposedly originated from external unauthorized data access (through hacking), but we don't know if anyone actually bought them (Techtarget, 2016). Connected to all these problems is the concept of doxing. Doxing is the act of publishing personal information about individuals online with the purpose of intimidating them. Doxing could violate both confidentiality, if the information is from a system with limited access, and privacy if it is connected to personal information. The term comes from the hacker culture where "dropping documents" or "dropping dox" connected to individuals was a way of making them lose the anonymity they had behind their hacker name. The phenomenon first emerged in the early 1990s, in Bulletin Board Systems and the early Internet, but has now spread and is quite common (Douglas 2016). It can be compared to writing a person's phone number on the wall of a public toilet, but doing this on thousands of toilet walls at the same time. Doxing could be very problematic if someone would use stolen or leaked medical records which often contain information that we consider private. Doxing is also related to the concept "Personal information" discussed earlier, as it is a mixture of general information about a person (where the person lives et cetera), and more private information (what the person has done, which alias the person uses on the Internet). As explained earlier, leaks can occur from any information system, analog or digital. But in the Internet era, it is much easier to spread information than before. The medium (the Internet), and how easily the medium can transfer information, is in this case more important than the message (the personal information) to use McLuhan's famous expression (McLuhan 2003, p. 7, p. 253).

It is always hard to predict the future, but it certainly seems that the amount of information, both personal and other, will continue to grow. In turn this growth is likely to affect all parts of the CIA Triad, not in the least, as seen in my examples above, that of confidentiality. How we will deal with these problems of information security and information growth is something we must decide in the near future.

Bibliography

Andersson, Joakim (2016) "Anhörigas journaltillgång upp i högsta instans" Available online 2017-10-22.http://lakartidningen.se/Aktuellt/Nyheter/2016/12/Anhorigas-journaltillgang-upp-i-hogsta-instans/

Andress, Jason (2015) "The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice", Oxford: Syngress

Baker, Maria J, George, Daniel R & Kauffman, Gordon L (2014) "Navigating the Google Blind Spot: An emerging need for professional guidelines to address Patient-Targeted Googling", J Gen Intern Med 30(1):6–7

Beta Telelink (2017) "Unauthorized access", Available online 2017-06-06. http://itsecurity.telelink.com/unauthorized-access-2/

Brottsbalken (1962:700)

Brottets krönika (1954) "Biskopsbreven", Stockholm: Medéns Förlag ABC2 "Auto key versus domain key", Availabile online 2017-06-06. http://wiki.c2.com/?AutoKeysVersusDomainKeys

Douglas, David M (2016) "Doxing: a conceptual analysis", Ethics and information technology, 6/2016

Järpvall, Charlie (2016) "Pappersarbete – Formandet av och föreställningar om kontorspapper som medium", Lund: Lund University

Ludvigsson, Jonas F, Otterblad-Olaussen, Petra, Pettersson, Birgitta U, Ekbom, Anders (2009) "The Swedish personal identity number: possibilities and pitfalls in healthcare and medical research" European Journal of Epidemiology. 24:659–667

Luleå Tingsrätt, Verdict B1868-16, 2016-09-29

McLuhan, Marshall (2005) "Understanding Media – The Extension of Man" London: Routledge

Nilsson, Inga (2007) "Medicinsk dokumentation genom tiderna – En studie av den svenska patientjournalens utveckling under 1700-talet, 1800-talet och 1900-talet", Lund: Lund University

Nilsson, Sophia (2016) "Stora problem för vården i Uppsala efter kraschat journalsystem", Computer Sweden, Availabile online 2017-06-06. http://computersweden.idg.se/2.2683/1.664717/uppsala-journalsystem-krasch

Patientdatalag (2008:355)

Patientjournallag (1985:562)

Prop 2007/08:126 "Patientdatalag mm", Stockholm: Regeringen

Sandén, Ulrika (2012) "Sekretess och tystnadsplikt inom offentlig och privat hälso- och sjukvård – ett skydd för patientens personliga integritet" Uppsala: Iustus Förlag

SCB (2016) "Personnummer", Stockholm: Statistiska Centralbyrån

Smedberg, Staffan (2012) "Sverige" in Jörvall et al, Det globala minnet, Stockholm: Riksarkivet

SOU 1984:73 "Patientjournalen – Huvudbetänkande av journalutredningen"

SOU 2016:41 "Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommitén"

Stockholms Tingsrätt, Verdict B4093-15, 2016-10-27

Techtarget (2016) "Nearly 10 million hospital patient records for sale on dark net web market". Available online 2017-02-17. http://searchsecurity.techtarget.com/news/450299408/10-million-hospital-patient-records-up-for-sell-on-dark-web-market

Tweel van den, Jan G & Taylor, Clive R (2010) "A brief history of pathology: Preface to a forthcoming series that highlights milestones in the evolution of pathology as a discipline", Virchows Archiv, vol 457, issue 1

Vismann, Cornelia (2008) "Files – Law and Media Technology" Stanford: Stanford University Press

Wacks, Raymond (2015) "Privacy – A very short introduction", Oxford: Oxford University Press

The Encyclopedia Britannica was used to gain information regarding the history of the photocopier.