Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure

Tobias Dehling
dehling@wiso.uni-koeln.de

Ali Sunyaev
sunyaev@wiso.uni-koeln.de

Faculty of Management, Economics and Social Sciences, University of Cologne, Germany

Abstract

Health information technology can have positive impacts on healthcare delivery and is utilised for various applications. Patient-centred services are a special kind of health information technology and are designed to cater to patients' needs. They manage personal medical information and utilise such information to offer personalised, advantageous services as well as information for patients. Due to the sensitivity of medical information and the gravity of possible consequences, if medical information falls into the wrong hands, patient-centred services need to employ security measures to ensure the privacy of patients. The German Nationwide Health Information Technology Infrastructure (HTI), which is currently being established, could serve as a fit and proper foundation for securely offering patient-centred services. In this paper, we illustrate the past developments and current status of the HTI introduction with a focus on security aspects related to patient-centred services. We depict how security features of the HTI can be applied to improve secure provision of patient-centred services. Furthermore, we present additional security measures that should be implemented by providers of patient-centred services.

1. Introduction

Recent studies attest health information technology (HIT) positive impacts [1]. Information technology (IT) is utilised in healthcare for various purposes from process improvement to the creation of new innovative services. Such purposes are, for instance, prevention of medical errors [2], improvement of diagnosis [3] or enhancement of the management of emerging infectious diseases [4]. Another application of HIT are patient-centred services. Such services can, for example, support specialised tasks, like the self-management of chronic diseases [5], or common tasks, like providing information on the pharmaceuticals a patient is taking [6]. Patient-centred services are attractive for patients because they offer direct benefits for patients instead of indirect benefits like better informed medical professionals. A qualitative study in a U.S. community [7] shows that patients deem exchange of health information beneficial and expect it to be rewarding. Nevertheless, besides desiring the potential benefits, patients were concerned with security and privacy, expected to be asked for consent, and wanted to be informed about the consent process.

In Germany a nationwide health information technology infrastructure (HTI), also known as health telematics infrastructure [8], is currently being established. Simultaneously, German residents are issued an electronic health card (eHC) that replaces the previous insurance card. Beyond serving as an insurance card, the eHC offers functionality like identifying its owner or storing information. Since health insurance is mandatory in Germany, all German inhabitants will gradually be issued an eHC. However, establishment of the HTI and introduction of the eHC has fallen behind schedule, the launch process was restructured, goals were realigned, features deferred, specifications deprecated, et cetera. In short, the whole process has become complex, protracted, and confusing [9]. Nevertheless, the German HTI will be established within the coming years. In this paper, we illustrate the past developments and current status of the HTI introduction with a focus on security aspects related to patient-centred services. Once the HTI is operational, it will be a suitable foundation for offering such services.

The paper is structured as follows: In chapter 2 'Establishment Process of the German Nationwide Health Information Technology Infrastructure' we illustrate relevant past developments and the current status of the HTI introduction. In chapter 3 'Privacy and Security of Patient-Centred Services' we elucidate patient-centred services and associated needs for privacy and security. Privacy and security measures that will be provided by the HTI as well as additional desirable security measures are described in chapter 4 'Employment of Security Measures'. The measures are illustrated with a use-case. Finally, we conclude the paper in chapter 5 'Conclusion'.

2. German Nationwide Health Information Technology Infrastructure

Essential characteristics of the HTI and eHC are enshrined in law. The obligation to introduce the eHC is codified in SGB V[1] §291, details regarding the eHC are specified in SGB V §291a, and SGB V §291b requires the creation of an association that is responsible for establishing the underlying HTI.

2.1. Initial Intentions

Introduction of the eHC and establishment of the underlying HTI was scheduled for January 1st, 2006. Mandatory functionality of the eHC is the capability to provide the same information as the prior insurance card to be replaced (e.g. name, current address, insurance number), transfer of electronic prescriptions, and verification of entitlement to retrieve care in the European Union. This mandatory functionality needs to be accessible with or without HTI access and patients are obligated to use it. Additional functionality that requires consent of patients was envisioned: Storage of medical information and retrieval of relevant information in case of emergency (e.g. allergies), transfer of information between cooperating institutions involved in the same case, storage of information required to improve safety of pharmacotherapy, cross-case and cross-institutional documentation of a patient's medical history, and documentation of utilised services and associated cost. Besides the patient, only medical professionals are authorised to access the stored information and offered services. Medical professionals prove their entitlement to access a service/information on patients with a smart card [10], which is called health professional card (HPC). Another type of smart card, the secure module card (SMC), provides functionality similar to HPC functionality. SMCs are associated with institutions (e.g. a hospital or a pharmacy) instead of individual medical professionals. SMCs are provided in multiple versions. SMC-Bs are integrated into the hardware used to connect to the HTI. SMC-As can be used by employees that need access to eHC/HTI functionality/information at individual workplaces in the institution and provide less functionality than HPCs/SMC-Bs. They can be used to access information on eHCs and can, if necessary, be enabled to remotely access information provided by an HPC/SMC-B. With this approach the card management of larger institutions is delegated and central HTI authorities do not have to manage the access rights of every last employee at every institution. Statutory health insurances have SMCs similar to SMC-Bs. Further technical components that need to provide security functionality, like card readers or network connectors, have integrated SMCs as well. Except of the mandatory functionality/information, patients can at a moment's notice revoke their consent or access-permissions and let certain information be deleted. Services can only be accessed when medical professionals identify themselves with their HPC and patients simultaneously grant authorisation with their eHC or alternative accepted procedures.

In January 2005, the association responsible for the underlying HTI (gematik [10]), was founded. Associates of the gematik are associations of stakeholders, like physicians, statutory health insurances, or hospitals. Further stakeholders like patients, politicians, scientists, or practitioners have no voting power but are represented in an advisory board. The gematik is responsible to work out technical details and data structures, devise test and certification procedures, and issue certificates for suitable technical components.

2.2. Restructuring

In 2009/2010 it became clear that the introduction process of the eHC/HTI required restructuring[2]. The project had deviated from the initial vision and project focus had changed to technical details instead of the creation of benefits for patients and medical professionals. In order to realign the introduction process with its initial objectives, it had to be assessed whether planned eHC functionalities are actually suitable to improve the quality of care and whether their implementations do not disproportionately burden medical professionals with additional effort. Inconsistent requirements of different stakeholders led to further effort and resource requirements for HTI establishment. In combination with the tight schedule, this raised the time pressure even more and led to the development of impractical processes and crude technical components.

To ease establishment of the HTI complexity was reduced. At first, only steps necessary to provide eHC offline functionality (i.e. functionality without HTI access) will be executed (base rollout); that is, equipping medical professionals with readers for eHCs and distributing eHCs to insurees. Once the base rollout is completed and tested, essential functionality will be implemented in seven individual projects that implement different aspects/services of the HTI (online rollout). Integration of further components will be tackled once the seven projects are completed, the HTI is operational, and stakeholders are satisfied with implementation, operation, and utilisation of the HTI. In charge of the projects are associates of the gematik that will bene-

1 Fifth social security code (In German: Fünftes Sozialgesetzbuch)

2 Corresponding official statements were made by associates of the gematik as well as the federal association of for information technology, telecommunications, and new media.

fit from them, in order to incorporate requirements of stakeholders/ensure that implementations fulfil stakeholders' needs. Furthermore, project leaders are required to inform other associates of the gematik regarding project progress and direction. The online rollout is split into two phases. In phase one, development of functionality for the administration of information regarding insurees is spearheaded by the National Association of Statutory Health Insurance (GKV-SV). The necessary infrastructure to facilitate the online verification of information on insurees stored on eHCs is contrived in a project led by the gematik; this infrastructure is called the 'preliminary infrastructure'. Besides functionality for the online verification of insuree information, the preliminary infrastructure additionally provides functionality for the management of qualified electronic signatures (QES[3]). In phase 2, further essential functionality is implemented in the five remaining projects. The German Medical Association is the project leader for an application that provides relevant information on patients in case of emergency. A project to facilitate the secure communication between care providers is led by the National Association of Statutory Health Insurance Physicians (KBV); this project will utilise the QES functionality established in the first step. The German Hospital Association is the project leader for the integration of an electronic case record with the HTI. To improve the safety of pharmacotherapy, management of patient-specific information regarding medication taken, prescriptions, treatment options, and undergone treatments is prepared by the Federal Union of German Associations of Pharmacists. Further development of the preliminary infrastructure to the target infrastructure, which provides collectively used services for all other projects, is managed by the GKV-SV and the KBV. Other functionality that was initially planned may be implemented later on.

Functional specifications of the projects, except for the pharmacotherapy safety project, were approved in a general meeting of gematik associates in March 2011; however, up until now[4], these are not publicly available. Currently, the corresponding technical specifications are being developed; most medical professionals and all hospitals are already equipped with eHC readers and eHCs are being distributed to the general population (70% of insurees have to be issued an eHC by the end of 2012). Splitting the online rollout into two phases (i.e. (1) preliminary infrastructure, (2) target infrastructure) was resolved in December 2011. Simultaneously the pharmacotherapy safety project was added to the second phase. Until the end of 2012 organisations who will instantiate and test the online rollout phase one will be selected and corresponding modalities clearly specified. At first the online verification of insuree information will be tested. QES has to be tested no later than 10 month afterwards. Accordingly, a nationwide utilisation of the HTI according to the online rollout phase one might be possible by the end of 2013/in 2014. Until the preliminary infrastructure of the HTI is established, eHCs provide only offline functionality. Like the previous insurance cards, they store relevant information on insurees. In contrast to prior insurance cards, they store information encrypted, feature a photo of the insuree to improve identification and verification of insurees, and they can be used as European insurance card – the respective information is provided on the back of an eHC.

3. Security of Patient-Centred Services

Patient-centred services are not a part of the HTI. Often they can also be characterised as value-added because they are not provided due to legal requirements; instead, they are provided to create additional value for their users; therefore, they can gain user acceptance and be financed[5]. Patient-centred services are designed to fulfil needs of patients, do not have to incorporate requirements of care providers, and can be provided by anyone who can finance the required resources. In principal, they can be provided independently of a care provider's information system (IS). Yet, interfacing with care providers might be useful to obtain information or utilise security functionality (e.g. HTI services). The services can provide any functionality patients deem useful; this might involve obtaining, accessing, storing, or managing medical information of patients, working on a local data basis, or any combination of these. Hence, patient-centred services are diverse and utilisation of patient information differs from service to service. A common trait is the creation of private, sensitive information. Some services that protocol aspects of a patient's health, like blood measurements of a diabetic, a medication intake protocol, or data measuring the fitness of an athlete, obviously store and create sensitive information. However, even services that do not store information create information. A malicious third party can gather information by only observing user behaviour. For example, a user accessing much information on heart medication could be considered more likely to have a heart disease than somebody reading about cough drops. While information related to patients ob-

3 A qualified electronic signature (QES) is a digital signature verifiably assigned to a single individual whose identity can be determined and issued by a certified certificate authority. A QES is by German law equivalent to a conventional written signature.

4 This research was conducted in the spring term of 2012.

5 Providers might, for instance, implement a pay-per-use model or profit from improving other factors like adverse drug reactions and benefit from less associated cost.

viously needs to be protected, the data basis necessary for a service to provide its functionality needs protection as well in order to ensure the reliability of provided information. Severity of consequences of privacy breaches differs from service to service and user to user. Additionally, not all threats can be foreseen. Still, patient-centred services should provide a basic degree of security to protect the privacy of patients. In the long run, this will not only benefit patients since these are more likely to choose trustworthy and secure services.

3.1. CIA Triad

A generally accepted foundation of information security is the CIA triad: Information security requires that the principles confidentiality, integrity and availability are upheld. Information systems need to ensure that only authorised users can access information (confidentiality). Stored information needs to be protected against unauthorised modification or deletion as well as irrevocable, accidental, and undesired changes by authorised users (integrity). Moreover, systems need to be accessible and fully operational whenever a user requires access to the system so that stored information and services can be retrieved and utilised when needed (availability). One might argue that the CIA triad is too general. The U.S. National Institute of Standards and Technology proposed, for instance, 33 more specific goals to achieve information technology security [11]. Nevertheless, in the focus of this paper the CIA triad can be deemed sufficient since we deal with the security of patient-centred services in general and the main asset deserving protection is the created/stored information. Specific and detailed security measures need to be tailored to individual, concrete services.

3.2. Potential Threats

As illustrated before, patient-centred services require confidentiality, integrity, and availability of information. Yet, it should be clarified against whom and what the information needs to be protected. A thorough assessment and classification of potential sources of and motivations for attack was presented in [12].

Potential sources of attack are, for example, hackers, script-kiddies, malicious insiders, organised crime, common malware, (cyber-) terrorists, or the media. These differ in characteristics like know-how, available resources, or expenditure of time. Hackers have, for instance, a lot of know-how and are willing to invest a rather high amount of time, but have little resources at hand. Organised crime has nearly unlimited resources and is willing to spend a lot of time for a large enough payout. Script-kiddies, on the other hand, are just toying around and have little know-how and resources. Malware might be written for an entire different purpose and cause damage by accident. Similarly, the motives for attack differ as well. Some attackers might act on financial incentives and others out of boredom or curiosity. A further motive is the intention to gain publicity or fame by causing damage or vandalism. Additionally, attackers might just want to discredit the system or demonstrate its inadequacy for some application.

4. Employment of Security Measures

An advantage of HTI utilisation for the provision of patient-centred services is that already existing, widely-used, and certified security functionality can be utilised. Besides savings in implementation efforts, utilisation of existing security functionality avoids potential sources of defects since service providers do not need to implement these security measures on their own. In the following, we will describe security measures provided by the HTI. Subsequently, we will address additional desirable security measures.

4.1. Security Measures Provided by the HTI

Information regarding the realisation of the HTI is mainly provided on the website of the gematik [10]. As illustrated in figure 1, the HTI uses a tiered architecture and features centralised and decentralised components. Centralised components, the backbone and the central systems, manage, for instance, the access to available mandatory and voluntary services. They verify corresponding access rights, compile logs for auditing, and ensure that the identity of patients is not known to the professional services. Professional services provide functionality like verification of insurance information or manage medical documentation. Virtual private networks (VPN) are used to secure network communication. Additionally, security gateways, consisting of packet filters and application level gateways, block not whitelisted traffic and link trusted networks. Decentralised components enable clients to connect to centralised parts of the HTI. Necessary functionality to utilise centralised parts of the HTI is provided by a device called connector. Connector functionality entails network connectivity, security functionality (e.g. encryption and signatures), and authentication of clients. To facilitate authentication functionality, card readers for HPC/SMC and eHC are hooked up to the connector so that access rights of the respective medical professional/institution can be verified and patients can confirm consent with their eHC. Furthermore, the connector has a module that represents application logic of professional services. This module serves as an interface for primary systems and establishes connections to professional ser-

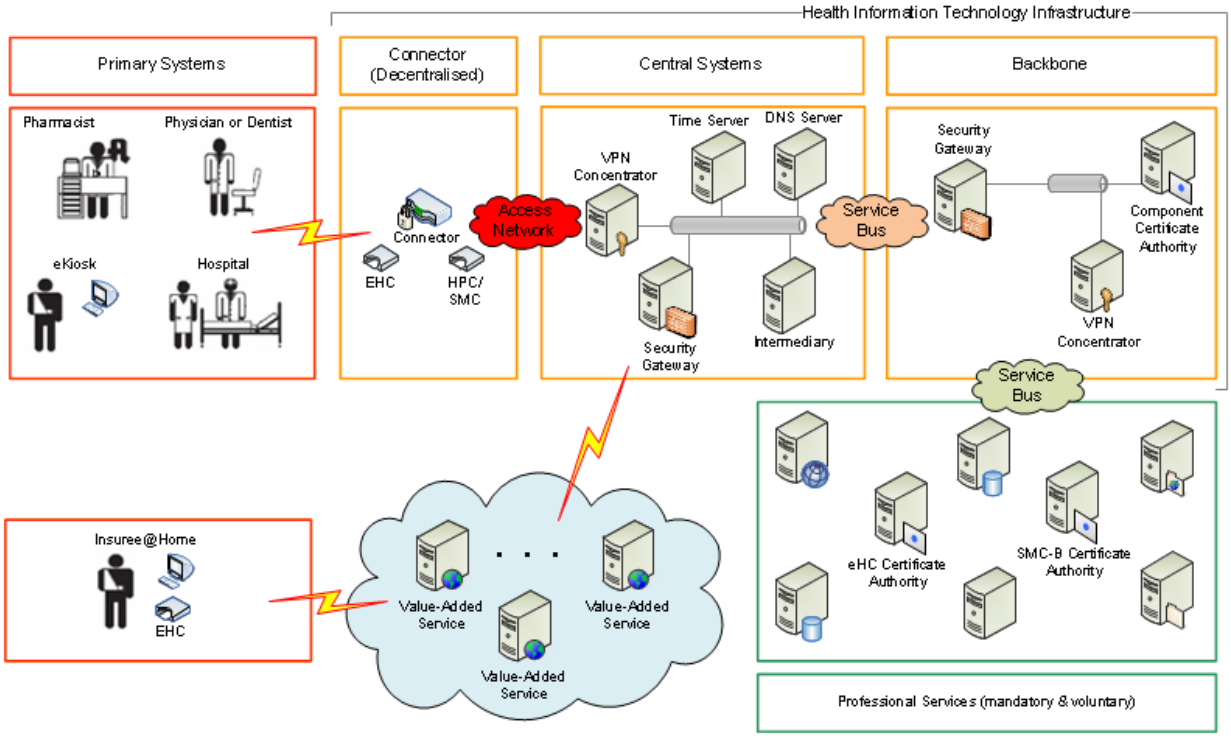

Figure 1: High-Level Architecture of German Health Information Technology Infrastructure (Adopted from [10]). Clients access the HTI from primary systems. The HTI consists of central and decentral components. Professional services are accessible via the HTI and patient-centred, value-added services can be accessed via the Internet and the HTI.

vices as well as connected card readers whenever necessary. If required, application logic for additional professional services can be loaded. Intermediaries handle communication between connectors and professional services, they locate services via DNS and pass packets unmodified to the respective services. Thus, they relieve other central components and professional services from traffic by concentrating many point-to-point connections in service buses. Clients can access HTI services from their primary systems. A primary system could, for example, be a hospital IS, a pharmacy IS, or a local IS in an office of a physician or dentist. Furthermore, clients can access further services, e.g., value-added services (VAS), provided by networks not included in the HTI, like the Internet. Corresponding traffic is routed through central security gateways that are extended with further capabilities like virus or malware detection. It should be taken into account that the architecture of the preliminary infrastructure, depicted in figure 1, might be adapted in the online rollout phase two. During the base rollout, medical professionals connect eHC readers directly to their primary systems in order to access offline functionality.

4.1.1. Access to HTI Security Measures

In contrast to professional services, VAS are not inspected by the gematik. However, to gain access to HTI services and be approved by the gematik, VAS need to verifiably demonstrate that their functionality corresponds to their specification, they employ sufficient measures to ensure information security, and that they do not endanger HTI services. HTI components are designed in such a way that information and configurations of newly approved VAS can be loaded upon approval. Hence, their keys can be registered with the Component Certificate Authority, they can be authorised in the security gateways, can be accessed via intermediaries et cetera. Approved VAS can access some functionality provided by the HTI: creation of secure communication channels with HTI components, authentication of signatures, signing, and encryption. Furthermore, functionality required by all offered services like creation and display of access logs for a patient's information will be centrally provided by the HTI. This saves effort for implementation and operation of VAS, avoids inconsistent individual implementations, and eases a consolidated provision of audit information.

To access value-added or professional services with the same level of security as medical professionals, patients need to use a primary system with connector access like an eKiosk. An eKiosk is a primary system that enables patients to utilise online HTI services on their own. They can, for example, be used to retrieve/modify personal information stored in the HTI or to verify that

one's privacy was not violated by checking who accessed information. While eKiosks might be sufficient to access professional services and VAS that are usually accessed at specific places like, for instance, offices of medical professionals, such primary systems are not useful to access patient-centred services. Requiring patients to visit dedicated locations in order to access a patient-centred service would most likely reduce user acceptance to a minimum. Patient-centred services should be available pervasively so that patients can access them whenever they need to. Thus, they need to be accessible via the Internet instead of from within the HTI. To improve security, patient-centred services can utilise eHC functionality in order to provide unambiguous identification or encrypt information. To utilise patient-centred services from a home computer, an eHC-compatible card reader featuring a keypad is required. A keypad is necessary to verify ownership of an eHC by entering a personal identification number (PIN).

Patients can access various information stored on their eHC from a home computer. Information regarding the insurance policy, eHC access logs, accrued charges for deductibles, or their public key can be read. Records specifying consent to voluntary services and personal decrees (e.g. consent to organ donation) can be read, activated, or deactivated. Links to utilised voluntary services can be read, updated, activated, or deactivated. Links to further information stored in VAS can be read, erased, activated, or deactivated. Furthermore, patients can use their eHC to authenticate signatures, compute digital signatures, and decipher encrypted documents.

4.1.2. Utilisation of HTI Security Measures

Since information regarding keys is stored on eHCs, eHCs provide functionality to ensure the confidentiality of personal medical information when using patient-centred services with public key cryptography [13]. Patients could encrypt information with their public key stored on their eHC and transfer it to a patient-centred service for save-keeping. Later on the information could be downloaded whenever necessary and decrypted with the private key. Benefits of using keys provided by the eHC are that, for security reasons, these are periodically exchanged and updated corresponding to contemporary, secure techniques. Currently 2048-bit RSA keys are used, which, as long as the private keys remain private, cannot be decrypted with current technology within a reasonable amount of time/money [14]. Ensuring the privacy of the private key is another merit of the eHC. Keys on eHCs are subject to secure, certified policies and processes during their whole life-cycle from generation to destruction. However, patient-centred services should be able to offer more than mere storage of information. Offering personalised information based on medical information leads to attractive and advantageous services for patients. For illustration, we propose the following example: A pregnant woman suffering from a cough could utilise a patient-centred service that proposes suitable prescription-free pharmaceuticals. She would specify known allergies, pharmaceuticals she is currently taking, and that she suffers from a cough and is pregnant; the patient-centred service would return a list of suitable cough medication that can be safely taken during pregnancy, does not cause respective allergic reactions and has no known adverse drug reactions with other pharmaceuticals the woman is taking.

Patient-centred services offering personalised information are also supported by eHC functionality. To ensure confidentiality, information send to the service could be encrypted with the service's public key and information returned from the service could be encrypted with the patient's public key. Additionally, both parties should sign transmitted information with their private key so that the authenticity can be validated by the receiving party. VAS can verify received, signed information through access to HTI public key infrastructure services and patients can verify signatures of VAS since the public key of the certificate authority (CA) that issues VAS certificates (i.e. the Component CA) are stored on issued eHCs. Once the authenticity of a service has been verified, the service's public key can be stored on the eHC for future use. This approach will also prevent man-in-the-middle attacks[6] since a third party cannot access transmitted information due to encryption and cannot sign injected instructions with valid signatures It is highly unlikely that modifications of transmitted packages will not invalidate the signatures [13].

In summary, keys and key management functionality provided by eHC and HTI can be utilised to improve the confidentiality of information. Integrity of information is improved during transfer. Contemporary, industry-strength encryption ensures the confidentiality of stored information. During transfer, encryption prevents privacy breaches and manipulation of the encrypted bitstream would invalidate signatures so that integrity breaches would be recognised.

4.2. Security Responsibilities of Providers

Utilisation of eHC/HTI security measures leads to some degree of security. However, providers of patient-centred services need to implement additional security measures in order to inhibit violations of a pa-

6 In a man-in-the-middle attack a malicious third party poses as the service from the user perspective and as as the user from the service perspective; this way communication can be sniffed, user instructions can be altered, or additional instructions can be added.

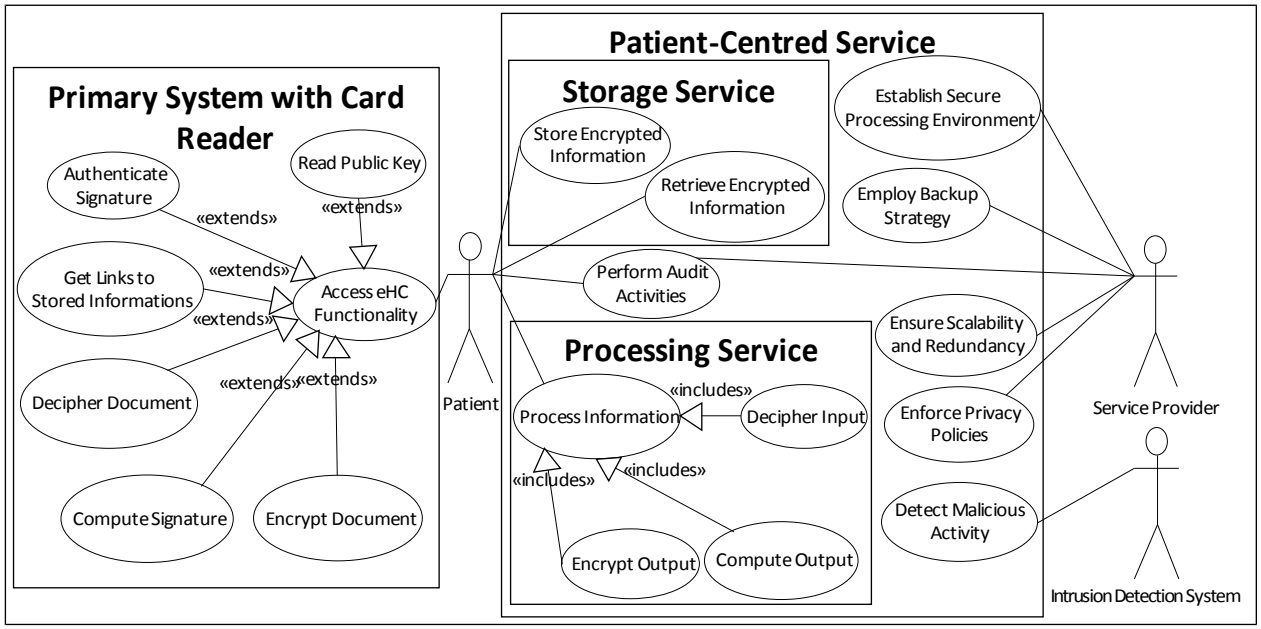

Figure 2: Use Case illustrating utilisation of patient-centred service and corresponding security measures. EHC functionality accessible to insurees at home as well as measures to protect information in patient-centred services are illustrated.

tient's privacy. Figure 2 illustrates the utilisation of a patient-centred service and the corresponding orchestration of HTI and service provider security measures with a use case. In the following, we will illustrate security responsibilities of service providers to uphold the principles of confidentiality, integrity, and availability.

4.2.1. Confidentiality

With eHC functionality information can be confidentially stored in patient-centred services [15]. The information can be encrypted so that it cannot be accessed by anyone but the patient. However, in order to obtain personalised services patients need to disclose information. Due to the employment of public key encryption, a service can link provided information to a patient's identity, which is associated with the public key. If providers of patient-centred services cannot be deemed trustworthy, it will be necessary to conceal the true identity of the patient from the service provider, so that a patient's information cannot be misused. This could be achieved by a trustworthy third party that handles communication with the service provider and strips all identity-related information from transmitted data. For the remainder of this paper we will assume that a provider of patient-centred services will not misuse a patient's information. This assumption will hold if either technical measures ensuring that information cannot be linked to the true identity of a patient are implemented or trustworthy handling of the information is more rewarding for the provider than misuse.

Since confidentiality of information is already maintained during transfer, service providers need only to preserve confidentiality when processing information. Information needs to be processed in a secure environment where unauthorised parties cannot access the information. In any other situation the information should be/remain encrypted in order to sustain confidentiality. In general, every single byte of information should be kept confidential. Even information that seems insignificant on its own can be used to infer privacy-violating information when linked with other sets of information; such links could, for instance, be established with data mining techniques [16]. If information contains, for instance, genetic information, even anonymised information can be reidentified [17]. Since having less information available reduces the amount of information that needs protection, service providers should practise data minimisation [18]; that is, request only information necessary for the service and delete information as soon as possible. This is also in the interest of patients because less meaningful information is less attractive for misuse. Consequently, patient-centred services should concentrate on user-friendly and secure ways to transfer necessary information instead of creating repositories for information retrieval in subsequent visits. Similarly, all users should always operate with minimal access rights so that users cannot cause issues in areas they do not even need to access. A further step would be to provide either a service that processes information or a service that stores information. This way, users could confidentially store as well as comfortably manage and administer their information in one service. Stored in-

formation could then be utilised in other services by transmitting only the relevant information. Such approach would ease provision of necessary information, but neither service would have access to valuable information. The storage service has no access to the encrypted information and the processing service has only temporary access to a small part of the information. Additionally, confidentiality breaches require much more criminal energy and ingenuity, if the data is not readily available and simple, spontaneous delicts, like running off with a hard disk, are unfruitful. Nevertheless, breaches of confidentiality in eHealth services are a reality and it is hard to completely regulate such services by law due to the dynamic and vicissitude of internet services [19]. Furthermore, it should be in the best interest of service providers to offer not only useful, but also secure and trustworthy services in order to gain user-acceptance. Hence, service providers should voluntarily adopt generally accepted recommendations, like the USAMC Policy Recommendations on Privacy [18], for maintaining the privacy of personal information. Besides following the minimisation principle, service providers should, for instance, solicit consent for utilising personal information, inform users on the utilisation of gathered information, let users view and correct accumulated information, utilise information in a traceable way, enforce respective policies, and train their personnel appropriately.

4.2.2. Integrity

In order to maintain integrity of information, employed algorithms and software need to work correctly and should not violate the integrity of information. Unintended modification/deletion by authorised users can be faced with appropriate backup strategies that allow unintended changes to be undone. It needs to be considered that a backup strategy can cause friction with confidentiality issues: If a patient wants to delete information, the information should irreversibly be deleted. Yet, it should be possible to restore the information, if it was deleted by accident. A possible solution might be to request confirmation when deleting information. A suitable backup strategy should be sufficient to protect the integrity of information from accidental, unintended changes. If changes of data are additionally logged and made available to patients, patients will be able to retrace modifications and undo undesired changes made by themselves or other authorised users. Encryption of data protects the integrity of information as well. If an encrypted record is deleted by a malicious, unauthorised user, it will be possible to restore the record from a backup. To prevent unauthorised modification encrypted records should additionally be signed with a private key, so that illicit modifications would invalidate the signature and can be detected/revoked. More serious problems can be caused if a malicious user manages somehow to manipulate the information in a way that cannot be detected as easily. Manipulations that, for example, cause a service to propose pharmaceuticals that patients are allergic to could cause a lot of harm. Since not every possible attack can be foreseen and a hundred per cent security level cannot be guaranteed, service providers need to employ mechanisms that detect undesired, malicious manipulations of/ actions in their services so that they can react appropriately and eliminate the vulnerabilities. Intrusion detection systems (IDS) provide such functionality. IDS monitor user actions in a system and raise an alarm, if they detect actions that seem to be of malicious intent or deviate from normal operation [20]. Besides virus and malware scanners, IDS systems might be able to identify systems infected with trojans[7] so that countermeasures can be initiated. Still, incompetent parties compromising their own systems by installing untrustworthy software pose a hard-to-manage thread. Further sources of integrity breaches, like technical failure, are handled by actions described in the next section.

4.2.3. Availability

Services that provide medical information need to offer high availability. To satisfy users, services need to be available whenever a user wants to use them. Moreover, patient-centred services provide medical information that might be of vital importance in case of an emergency. A patient should not waste precious time by having to try different services to obtain some important information. Hence, patient-centred services need to be designed with scalability and failure-tolerance (redundancy) in mind so that their performance output can be easily adopted to rising performance needs and tasks of failed technical devices are automatically assigned to alternate devices. Services providing medical information should especially avoid single points of failure and feature adequate redundancy. Simultaneously, confidentiality and integrity issues need to be considered since redundancy increases possible points of attack. On the other hand, redundancy increases the likelihood that security breaches do not compromise all viable parts of a system. Besides scalability and redundancy, the capability to defend against attacks that try to impair the availability of services, like denial of service (DoS[8]) attacks,

7 A trojan (horse) is a malicious software that poses as a useful tool so that users install it. Once installed, trojans enable attackers to compromise a system in a variety of ways.

8 DoS attacks, for example, “attempt to consume a server's resources (network bandwidth, computing power, main memory, disk bandwidth etc) to near exhaustion so that there are no resources left to handle requests from legitimate clients” [21].

should influence the design and architecture of patient-centred services. Such attacks can compromise the availability of an offered service; yet, if a service is appropriately designed even infamous DoS attacks can be warded off [21]. Services should strengthen their defence against DoS attacks through ingress filtering, so that outside packages with local addresses are discarded. Besides encryption and signatures, package filtering to sanitise traffic, as also conducted by the HTI security gateways, also represents a measure against spoofing attacks[9].

4.2.4. Additional Security Responsibilities

Besides focussing on confidentiality, integrity, and availability of patient-centred services, security measures that are generally required by software/web applications need to be employed during the whole life-cycle of an offered service; especially, in the implementation, testing and deployment phases [22], [23]. Software developers should enforce input validation, hotspot protection, and output validation. Applications should "consider all inputs malicious until proven otherwise" [22], in order to ward off potential attacks. Hotspots, like a database, demand special attention to protect, for instance, against SQL injections[10]. Application output needs to be validated as well so that applications cannot send unintended information. In the testing phase, the application needs to be tested for vulnerabilities in addition to fulfilment of functional requirements. Besides improving defence against wide-spread vulnerabilities like SQL injections or Cross-Site Scripting (XSS[11]) attacks [22], [23], such general security measures eliminate possible points of attack. Moreover service providers should not rely on single actions but employ complementing techniques to improve detection and elimination of possible vulnerabilities and make it more difficult to attack the service. However, technical measures cannot protect against all kinds of attack. Attacks that use, for example, social engineering techniques like phishing attacks[12] target users instead of the system itself [24]. Correspondingly, it is important that users and personnel are appropriately trained, informed, and able to identify possible threats. In the end, users and most employees are not security experts and cannot be expected to behave adequately in every situation. Technical measures, design decisions, and efforts to rise awareness need to be fittingly mixed and applied.

9 In spoofing attacks attackers use falsified sender information (e.g. in IP packets) to pose as a trusted host or conceal their identity.

10 SQL injection refers to SQL code that is given as application input by a malicious user, executed by the application, and intended to gain access to the database or tamper with the data.

11 XSS attacks exploit not sanitised input to insert scripts which are stored by the web page and executed, due to not sanitised output, when other user access the web page [23].

12 For phishing "criminals use spoofed email messages to trick people into sharing sensitive information or installing malware" [24].

5. Conclusion

While patient-centred services can be beneficial for patients and offer personalised information and functionality, information security aspects must be considered. Patient-centred services utilise, store, and create sensitive medical information. In order to ensure the security of patient-centred services the principles of confidentiality, integrity, and availability need to be upheld.

In Germany, a nationwide health information technology infrastructure is currently being established. Since initial project objectives could not be met and the establishment process of the HTI fell behind schedule, the project was restructured and realigned with the initial goals. Currently, the HTI provides only offline functionality. Insurees are being issued eHCs and information on these can be read with corresponding card readers. In the next phase, the basic infrastructure will be introduced so that a nationwide network that offers medical services and information will be available to medical professionals/institutions and patients. Since this network entails extensive security measures it can be used as a suitable foundation for securing patient-centred services. Due to key management processes and policies of the HTI, private and public keys stored on eHCs can be used to ensure confidentiality of information stored in patient-centred services and improve confidentiality and integrity while transferring information from/to services. With a rising project progress and associated information, more detailed information on the utilisation of HTI functionality to secure patient-centred services will be made available.

However, providers of patient-centred services need to employ further measures to protect the privacy of patients who use patient-centred services. In order to maintain confidentiality of information, patient-centred services should not know the true identity of their users, enforce the minimisation principle and utilise available information only in secure environments. Instead of creating repositories of information, service providers should focus on offering secure methods for users to specify relevant information. Security will be improved, if patient-centred services either store or process medical information. Integrity of information can be improved by employing software that works correctly, appropriate backup strategies as well as encryption and signatures. Since information provided by a patient-centred service may be of vital importance, services need to be available whenever a patient wants to access them. Hence, they need to be designed with

scalability and failure-tolerance in mind. Moreover, patient-centred services need to implement security measures generally required by software/web applications in order to increase the likelihood to ward off attacks.

All in all, security is an important aspect when offering patient-centred services. Providers of patient-centred services need to implement appropriate security measures to protect the privacy of personal, sensitive, medical information of their users. Security measures implemented by the HTI, which is currently being established in Germany, can be utilised to improve the security of patient-centred services. The HTI can serve as a foundation for securing patient-centred services. However, in the end, patients need to weigh up the benefits and risks of using such services on their own. Service providers need to master the challenge of designing offered services in such a way that patients decide in their favour.

References

[1] M.B. Buntin, M.F. Burke, M.C. Hoaglin and D. Blumenthal. "The Benefits Of Health Information Technology: A Review Of The Recent Literature Shows Predominantly Positive Results," Health Affairs, vol. 30, pp. 464-471, Mar. 2011.

[2] R. Aron, S. Dutta, R. Janakiraman and P.A. Pathak. "The Impact of Automation of Systems on Medical Errors: Evidence from Field Research," Inform. Syst. Res., vol. 22, pp. 429-446, Sep. 2011.

[3] N. Savage. "Better Medicine Through Machine Learning," Commun. ACM, vol. 55, pp. 17-19, Jan. 2012.

[4] Y. Chen, S.A. Brown, P.J. Hu, C. King and H. Chen. "Managing Emerging Infectious Diseases with Information Systems: Reconceptualizing Outbreak Management Through the Lens of Loose Coupling," Inform. Syst. Res., vol. 22, pp. 447-468, Sep. 2011.

[5] A. Sunyaev and D. Chornyi. "Supporting Chronic Disease Care Quality: Design and Implementation of a Health Service and its Integration with Electronic Health Records," ACM J. Data Inf. Qual., vol. 3, May 2012, article 3.

[6] T. Dehling and A. Sunyaev. "Architecture and Design of a Patient-Friendly Web Application Offering Information in Patient Information Leaflets and Supplementary Services", in Proceedings of the Eighteenth Americas Conference on Information Systems, Seattle, Washington, U.S., 2012.

[7] S.R. Simon, J.S. Evans, A. Benjamin, D. Delano and D.W. Bates. "Patients' attitudes toward electronic health information exchange: qualitative study," Journal of Medical Internet Research, vol. 11, Jul. 2009. http://www.jmir.org/2009/ 3/e30.

[8] A. Schweiger, A. Sunyaev, J.M. Leimeister and H. Krcmar. "Information Systems and Healthcare XX: Toward Seamless Healthcare with Software Agents," Comm. Assoc. Inform. Syst, vol. 19, 2007, pp. 692-709.

[9] A. Tuffs. "Germany puts universal health e-card on hold," BMJ, vol. 340, 2010, pp. c171.

[10] Gematik. "Specifications and further inf. (in German)," Internet: www.gematik.de, [Apr. 05, 2012].

[11] G. Stoneburner, C. Hayden and A. Feringa. (2004, June). Engineering Principles for Information Technology (A Baseline for Achieving Security). 800(27). http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf [Apr. 03, 2012]

[12] A. Sunyaev, M.J. Huber, C. Mauro, J.M. Leimeister and H. Krcmar. "Bewertung und Klassifikation von Bedrohungen im Umfeld der elektronischen Gesundheitskarte (English: Assessment and Classification of Threats around the eHC)," in Proc Informatik 2008, Munich, Germany, 2008, pp. 65-70.

[13] M.E. Hellman. "An Overview of Public Key Cryptography," IEEE Communications Society Magazine, vol. 16, pp. 24-32, Nov. 1978.

[14] T. Kleinjung, A.K. Lenstra, D. Page and N.P. Smart. "Using the Cloud to Determine Key Strengths," Internet: http://eprint.iacr.org/2011/254.pdf, May 23, 2011 [Apr. 05, 2012].

[15] A. Kaletsch and A. Sunyaev. "Privacy Engineering: Personal Health Records in Cloud Computing Environments," presented at ICIS 2011, Shanghai, China, 2011.

[16] L. Brankovic and V. Estivill-Castro. "Privacy Issues in Knowledge Discovery and Data Mining," in Proceedings of Australien Institute of Computer Ethics Conference (AICEC99), Melbourne, Australia, 1999, pp. 89-99.

[17] J.E. Lunshof, R. Chadwick, D.B. Vorhaus and G.M. Church. "From genetic privacy to open consent," Nature Reviews Genetics, vol. 9, pp. 406-411, May 2008.

[18] US Public Policy Council of the Association for Computing Machinery. "USAMC Policy Recommendations on Privacy," Internet: http://usacm.acm.org/privsec/category.cfm?cat=7, [Apr. 06, 2012].

[19] J. Goldman and Z. Hudson. "Virtually Exposed: Privacy and E-Health, " Health Affairs, vol. 19, pp. 140-148, Nov. 2000.

[20] S. Axelsson. "Intrusion Detection Systems: A Survey and Taxonomy," Internet: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.83.3043, Mar. 14, 2000 [Apr. 06, 2012].

[21] M. Srivatsa, A. Iyengar, J. Yin and L. Liu. "A Client-Transparent Approach to Defend Against Denial of Service Attacks," in Proceedings of the 25th Symposium on Reliable Distributed Systems (SRDS '06), Leeds, U.K., 2006, pp. 61-70.

[22] N. Antunes and M. Vieira. "Defending against Web Application Vulnerabilities", IEEE Computer, vol. 45, pp. 66-72, Feb. 2012.

[23] L.K. Shar and H.B.K. Tan. "Defending against Cross-Site Scripting Attacks," IEEE Computer, vol. 45, pp. 55-62, Mar. 2012.

[24] J. Hong. "The State of Phishing Attacks," Commun. ACM, vol. 55, pp. 74-81, Jan. 2012.