German Health Information Technology Infrastructure: A Large-Scale Network Offering Support for Software Engineering in Health Care

Tobias Dehling, Ali Sunyaev
Faculty of Management, Economics and Social Sciences
University of Cologne
Cologne, Germany
{dehling,sunyaev}@wiso.uni-koeln.de

***Abstract*—A central health information technology infrastructure (HTI) can alleviate software engineering challenges in health care by serving as a central hub for health care applications and stakeholders. We shortly introduce establishment process of as well as information and services provided by the German HTI to encourage putting the inclusion of HTI features in health IT software engineering projects under consideration and to offer an insight into one of the largest health IT projects in the world.**

***Index Terms*—health information technology, health IT, infrastructure, network, telematics, Germany, patient-centered, eHealth, health, health care, electronic health card, health professional card, software engineering, applications**

I. Introduction

The introduction of a nationwide health information technology infrastructure (HTI) in Germany is one of the largest health IT projects in the world. Similar to other international initiatives like HIPAA/HITECH in the US [1] or the Japanese Community Medicine Recovery Plan [2], the project tries to leverage benefits of large-scale health information technology networks to improve quality and save cost in health care. Additionally, a central HTI can serve as tool for health IT software engineering.

Information technology is used in health care for various purposes from process improvement to the creation of new innovative services. Such purposes are, for instance, prevention of medical errors [3], improvement of diagnosis [4] or enhancement of the management of emerging infectious diseases [5]. Further health IT applications are directly tailored to patients' needs and support, for example, specialized tasks like the self-management of chronic diseases [6] or more common tasks like providing information on the pharmaceuticals a patient is taking [7].

From the perspective of software engineering, development of health IT applications is challenging [8]. Many stakeholders have to be considered. Old-fashioned established processes need to be reengineered or incorporated into new systems. Complex medical relationships might need to be modeled. Errors should not happen since lives are at stake and the access to security-sensitive health information creates high demand for protection of information security and privacy. A HTI can alleviate such challenges by serving as a central hub for health IT applications. Hence, health IT software engineers do not have to implement all required functionality on their own and can leverage HTI functionality instead. A common foundation leads to further synergies: All clients could, for instance, benefit from tests and improvements of the centralized components and the functionality offered by the centralized components can be implemented and maintained by specialized experts. Furthermore, research and insights from various fields can be consolidated and incorporated into the HTI. In this paper, we shortly present establishment and features of the German HTI to give an insight into one of the largest worldwide health IT projects and to encourage putting the inclusion of HTI features in health IT software engineering projects under consideration. While the HTI establishment process has to face many software challenges, we focus on the potential of HTI to alleviate software engineering challenges in health care: We shortly introduce the overall establishment process of the German HTI and present HTI functionality and services, the architecture of the German HTI as well as possibilities to leverage HTI functionality, information, and services in health care software engineering. A more detailed description of the German HTI with a focus on leveraging information security and privacy features of the HTI in patient-centered health IT services can be found in [9].

The HTI (in the remainder of this paper the term HTI refers to the German HTI) introduction is an ambitious, expensive, and protracted project [10]. Seven years after the initially targeted date for HTI introduction (2006), the project is still ongoing; however, many hurdles (e.g. stakeholder conflicts, project management issues, obsolescence of technical components) have been taken and the first changes of the project are rolled out to the general population [9]. By the end of 2012, 70% of German insurees had to be issued a smart card (called electronic health card (eHC)) that replaces the previous insurance card and enables patients to access HTI functionality. Since health insurance is mandatory in Germany, all German inhabitants will gradually be issued an

eHC. At first, a basic preliminary infrastructure implementing functionality required for online verification of insuree information will be established. Subsequently, the preliminary infrastructure will be adjusted and extended to host the functionality envisioned for the target infrastructure. The HTI represents an inter-organizational network that connects all stakeholders, e.g. 2,200 hospitals, 123,000 general practitioners, 21,000 pharmacies, 80,000,000 patients [10], of the health care system over the internet. Accordingly, the HTI offers functionality to support all stakeholders and employs security measures and services to protect offered functionality and communication.

II. HTI Functionality and Services

Information regarding the realization of the HTI is mainly provided on the website of the gematik (the association responsible for the HTI) [11]. At first, only steps necessary to provide 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 (online rollout). Integration of further components will be tackled once the online rollout is completed, the HTI is operational, and stakeholders are satisfied with implementation, operation, and use of the HTI.

The online rollout is split into two steps. In step one, functionality for the administration of information regarding insurees is developed. This requires also the establishment of the infrastructure necessary to facilitate the online verification of information on insurees stored on eHCs; this infrastructure is called the preliminary infrastructure. In addition to the functionality for online verification of insuree information, functionality for the management of qualified electronic signatures (a digital signature verifiably assigned to a single individual, whose identity can be determined, issued by a certificate authority; by German law, a qualified electronic signature (QES) is equivalent to a conventional written signature) is provided by the preliminary infrastructure. At the beginning of 2013 the base rollout is nearing completion and functionality of the online rollout step one is being tested.

Besides the patient, only medical professionals are authorized to access information stored on eHCs and HTI services. Medical professionals prove their entitlement to access a service/information on patients with a smart card called health professional card (HPC). Secure module cards (SMC) provide functionality similar to HPC functionality, but 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 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 authorization with their eHC or alternatively accepted procedures.

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.

In step 2 of the online rollout, further essential functionality is implemented. In case of emergency information will be stored on eHCs. Secure communication channels between health care providers will be established; this feature will use the QES functionality established in the first step. Functionality to manage electronic case records across involved medical professionals and institutions will be made available. To improve the safety of pharmacotherapy, patient-specific information regarding medication taken, prescriptions, treatment options, and undergone treatments will be managed within the HTI. Furthermore, the preliminary infrastructure will be extended to the target infrastructure to offer services collectively used by other features.

III. HTI Architecture

The HTI uses a tiered architecture and features centralized and decentralized components, as depicted in Fig. 1. Centralized 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 communications. Additionally, security gateways, consisting of packet filters and application level gateways, block not whitelisted traffic and link trusted networks. Decentralized components enable clients to connect to centralized parts of the HTI.

Necessary functionality to access centralized 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

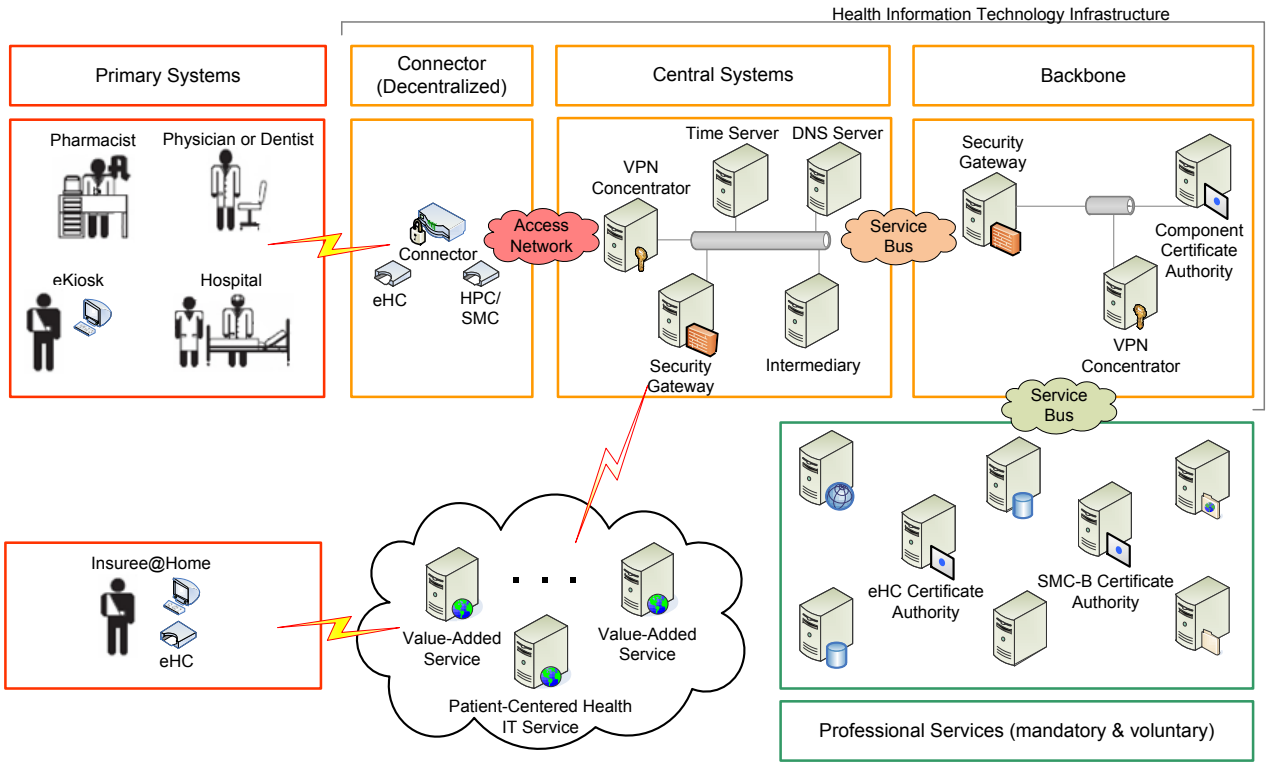

Fig. 1: High-level architecture of German HTI (adapted from [11]). Clients access HTI information and HTI services from their primary systems. The HTI consists of centralized and decentralized systems. Via security gateways services from external networks can be integrated with the HTI.

connections to professional services 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, 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 Fig. 1, might be adapted in the online rollout step two. During the base rollout, medical professionals connect eHC readers directly to their primary systems in order to access offline functionality.

IV. Access to HTI Information and Services

All systems that have access to a connector can use HTI services and functionality via the interfaces offered by connectors. Hence, all systems at medical institutions or offices of medical professionals can access HTI information and services. The connector will handle security details like verifying authorization by checking the required smart cards and encrypting traffic. It is also possible to integrate developed health care applications directly into the HTI so that they can be offered as a professional service. Such services will be approved and checked in detail by the gematik and have to undergo certification and verification procedures. During the online rollout the integration of an electronic case record with the HTI will pilot and shape this approval process.

An alternative method to access HTI information and services from a health care application is deploying the application to an external network like the internet and registering the application with the HTI as a VAS. While VAS cannot access as much HTI features as professional services they can simultaneously offer interfaces to users that do not have access to a connector. Hence, VAS represent a type of service between applications without HTI access and professional services. 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 authorized 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 access 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. Requiring patients to visit dedicated locations in order to access a VAS would most likely reduce user acceptance. VAS can however also be accessed over the internet from home computers. Such communications could be protected by common mechanisms (e.g. SSL encryption, multi-factor authentication), but could also be enhanced by eHC functionality in order to provide unambiguous identification or encrypt information and communication.

To access VAS from a home computer while employing eHC functionality, 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. 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 used voluntary services can be read, updated, activated, or deactivated. Furthermore, patients can use their eHC to authenticate signatures, compute digital signatures, and decipher encrypted documents.

Thus, while the HTI offers multiple access points where HTI services and information can be leveraged in health care software engineering, the eHC alone is not only a safe storage for patient information, but also like a Swiss army knife for patient-focused security features.

V. Conclusion

To sum up, the HTI is one of the largest health IT projects in the world and offers a multitude of information and services. These can be used in various ways in health care software engineering projects. Therefore, the HTI can alleviate at least some challenges of software engineering by serving as a central nationwide hub for health care applications and stakeholders. Thus, the HTI is rather a collection of tools that can be employed for various purposes and to alleviate challenges in health care software engineering. While it is not likely that something like the HTI will be available on a global scale in the near future, it is definitely worth considering other initiatives in the application environment during health care software engineering projects to benefit from standardized, centralized components and leverage associated synergies. In the coming years, personal health records [12] may rise to a central hub for global safekeeping and access to personal health information, but the HTI goes even further, at least on a national level.

References

[1] M. Delgado, "The Evolution of Health Care IT: Are Current U.S. Privacy Policies Ready for the Clouds?," in 2011 IEEE World Congress on Services, Washington, DC USA, 2011, pp. 371–378.

[2] C. Abraham, E. Nishihara, and M. Akiyama, "Transforming Healthcare with Information Technology in Japan: A Review of Policy, People, and Progress," International Journal of Medical Informatics, vol. 80, no. 3, pp. 157–170, Mar. 2011.

[3] R. Aron, S. Dutta, R. Janakiraman, and P. A. Pathak, "The Impact of Automation of Systems on Medical Errors: Evidence from Field Research," Information Systems Research, vol. 22, no. 3, pp. 429–446, Sep. 2011.

[4] N. Savage, "Gaining Wisdom from Crowds," Communications of the ACM, vol. 55, no. 3, pp. 13–15, 2012.

[5] Y.-D. Chen, S. A. Brown, P. J.-H. Hu, C.-C. King, and H. Chen, "Managing Emerging Infectious Diseases with Information Systems: Reconceptualizing Outbreak Management Through the Lens of Loose Coupling," Information Systems Research, vol. 22, no. 3, pp. 447–468, Sep. 2011.

[6] 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 Journal of Data and Information Quality, vol. 3, no. 2, pp. 3:1–3:21, May 2012.

[7] T. Dehling and A. Sunyaev, "Architecture and Design of a Patient-Friendly eHealth Web Application: Patient Information Leaflets and Supplementary Services," in Proceedings of the 18th Americas Conference on Information Systems, Seattle, Washington, U.S., 2012, Paper 5.

[8] C. Pagliari, "Design and Evaluation in eHealth: Challenges and Implications for an Interdisciplinary Field," Journal of Medical Internet Research, vol. 9, no. 2, e15, 2007.

[9] T. Dehling and A. Sunyaev, "Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure," in Proceedings of the 3rd USENIX Workshop on Health Security and Privacy (HealthSec'12), Bellevue, WA, U.S., 2012.

[10] A. Tuffs, "Germany Puts Universal Health e-Card on Hold," British Medical Journal, vol. 340, no. 1, p. c171, Jan. 2010.

[11] Gematik, "Gematik homepage offering HTI specifications and further information (in German)," 2010. [Online]. Available: http://www.gematik.de. [Accessed: 12-Feb-2013].

[12] I. Carrión, J. L. F. Aleman, and A. Toval, "Personal Health Records: New Means to Safely Handle Health Data?," Computer, vol. 45, no. 11, pp. 27–33, 2012.