Challenges in eHealth: From Enabling to Enforcing Privacy

Naipeng Dong*, Hugo Jonker, and Jun Pang

Faculty of Sciences, Technology and Communication,
University of Luxembourg, Luxembourg

Abstract. Privacy is recognised as a fundamental requirement for eHealth systems. Proposals to achieve privacy have been put forth in literature, most of which approach patient privacy as either an access control or an authentication problem. In this paper, we investigate privacy in eHealth as a communication problem, since future eHealth systems will be highly distributed and require interoperability of many sub-systems. In addition, we research privacy needs for others than patients. In our study, we identify two key privacy challenges in eHealth: *enforced privacy* and *privacy in the presence of others*. We believe that these privacy challenges are vital for secure eHealth systems, and more research is needed to understand these challenges. We propose to use formal techniques to understand and define these new privacy notions in a precise and unambiguous manner, and to build an efficient verification framework.

1 Introduction

The inefficiency of traditional paper-based health-care and the development of information communication technologies, in particular cloud computing, mobile, and satellite communications, give electronic health-care (eHealth for short) a great opportunity to grow as an important part of people's daily life. eHealth systems aim to provide effective support for secure sharing of information and resources across different health-care settings, and workflows among different health-care providers. The services of such systems for the general public are intended to be more secure, more effective, more efficient, more patient-centered and more timely. However, the attractive advantages of eHealth systems entail many scientific challenges. One of the foremost of these are the privacy issues raised by adapting electronic storage and communication, due to the sensitive nature of health data. Indeed, privacy in eHealth has been recognised as one of the paramount requirements necessary for adoption by the general public [1, 2]. Moreover, existing privacy experience from domains such as electronic voting (e.g., [3]) and online auctions (e.g., [4]) does not carry over straightforwardly. In voting and auctions, there is a natural division into two types of roles: participants (voters, bidders) and authorities (who run the election/auction). eHealth systems have to deal with a far more complex constellation of roles: doctors,

* N. Dong was supported by the grant No. PHD-09-027 from FNR Luxembourg.

patients, pharmacists, insurance companies, medical administration, etc. Each of these roles has access to different private information and different privacy concerns. As existing privacy approaches from other domains are not properly equipped to handle such a diverse array of roles, privacy must be tailored to the health-care domain.

Various proposals to achieve privacy in eHealth have been put forth in the literature. Most focus on patient privacy (notable exceptions: [5–7]) and approach that as an access control or authentication problem. The virtually exclusive focus on patient privacy in the literature has left the question of privacy requirements of other parties, doctors in particular, wide open. The fact that some parties, e.g., pharmacists, cannot be fully trusted adversely impacts privacy [6].

Furthermore, eHealth systems must provide assurance of privacy and address privacy issues at different system levels – architectural design, access control, communication protocols, etc. Making the issue more complex is the sensitive nature of health-care data, which is subject to regulations, guidelines and application of professional ethics. Currently, (patient) privacy is usually described in terms of protection of information and in terms of controlling access to services. Thus, it is commonly achieved in practice by means of a form of access control or authentication (e.g., see [8–12]). However, typical eHealth systems, especially in future, will be highly distributed and require interoperability of many subsystems. Even if health-care data is well protected and access control is perfectly employed, improperly designed communication protocols for such interoperability will cause information leakage and hence breach users' privacy. So far, security and privacy of communication protocols in eHealth systems is seldom studied in the literature. This implies that related privacy notions, emerging in other fields, do not yet have a counterpart in the eHealth domain. A prime example is the notion of coercing vs. enforced privacy: in voting, a voter is coerced to reveal how she voted (to sell her vote). For eHealth systems, a similar case would be a pharmaceutical company bribing a doctor to reveal which medicine he prescribed. Given the current state of eHealth research, we find that *enabling* privacy is well-studied. However, there is a lack of attention for *enforcing* privacy.

Contributions. Our main contribution is to identify two new types of enforcing privacy as key privacy challenges for the field: *enforced privacy* (e.g., a doctor cannot prove to a pharmaceutical company which medicine he prescribed) and *privacy in the presence of others* (e.g., a patient cannot reveal which doctor prescribed her medicine). We propose to use formal techniques to address these challenges, that is: to understand and interpret these new privacy notions in a precise and unambiguous manner, and to build an efficient verification framework for analysing privacy properties of eHealth systems.

Outline of the paper. We briefly survey existing approaches to privacy in eHealth in Section 2, finding a lack of attention to enforced privacy. Next, Section 3 identifies what we argue to be two main challenges for privacy in eHealth. In the remainder of the paper, we outline the need for a formal approach in addressing these challenges (Section 4), and report briefly on our ongoing analysis of an eHealth protocol claiming to be privacy-preserving (Section 5).

2 A brief survey of privacy in eHealth

Privacy in eHealth systems has attracted much research effort and a variety of different privacy-enabling methods have been proposed. This section provides a brief overview[1] of previous work on privacy in eHealth. We divide previous work in two categories, focusing on patient privacy (Section 2.1) and on doctor privacy (Section 2.2), respectively.

2.1 Enabling patient privacy

The importance of patient privacy in eHealth is traditionally seen as vital to establishing a good doctor-patient relationship. This is even more pertinent with the emergence of the Electronic Patient Record [8]. As in most of the literature, a necessary early stage of eHealth is to transform the paper-based health-care process into a digital process. The most important changes in this stage are made to patient information processing, mainly health-care records. To properly express privacy requirements for such patient records, privacy policies are considered the de facto standard. There are three main approaches to implement these requirements of patient privacy: access control, architectural design, and the use of cryptography.

Patient privacy by access control. To preserve privacy of electronic health-care records, one necessary part is to limit access to these records to allowed parties. Anderson [8] lists several privacy threats to personal health information as support for his claim that privacy policies for access control should be mandatory in eHealth systems. Anderson [8] proposes access rules to restrict the number of users who can access any record and the maximum number of records accessed by any user. In a case study [9], Louwerse argues that consent-based access rules (e.g., a patient approving use of his data for research) are required in addition to rules based on the "need-to-know" principle. Evered and Bögeholz [11] investigate minimal-disclosure access constraints for a small eHealth system, and find that even for a small system, constraints cannot be expressed easily or clearly using static access rules. As a solution, they propose adding a middle layer of logic, which translates constraints into access rules. Reid et al. [10] adapt role-based access control (RBAC) to include explicit consent and denial. Explicit denial is to grant access to a role (e.g., doctors), but deny access to a particular individual (excluding a particular doctor); explicit consent is the converse property: granting access for individuals while denying access to the role. Kalam et al. claim also investigate shortcomings of classical access control models (such as RBAC and task based authorisation controls (TBAC) [13],

[1] This literature overview is not intended to be exhaustive.

etc.), and find these are insufficient to capture security policies that need to be context-aware (e.g., to grant emergency access to a patient record), that specify onligations or recommendations. They propose a new access control model OrBAC [14] (organisation based access control), designed to be particularly suited for eHealth access control. The access rules of eHealth systems are complex, and may become inconsistent – one rule may contradict another. Cuppens et al. [15] propose assigning priorities to rules and show that this can resolve such problems in rule-based access control and in OrBAC.

Patient privacy by architectural design. As stated in the introduction, eHealth systems cater to a number of different roles, including doctors, patients, pharmacists, insurers, etc. Each such role has its own sub-systems or components. As such, eHealth systems can be considered as a large network of systems, including administrative system components, laboratory information systems, radiology information systems, pharmacy information systems, and financial management systems. Diligent architectural design is an essential step to make such a complex system function correctly. Since privacy is important in eHealth systems, keeping privacy in mind when designing the architecture of such systems is a promising path towards ensuring privacy [16]. Ko et al. [17] discuss privacy issues when building wireless sensor networks for eHealth. Some eHealth system architectures are specially designed with a particular privacy issue in mind, e.g., Maglogiannis et al. [18] propose an architecture that enhances patient location privacy by communication via proxies, which can learn location but not patient identity. There also exist architectures which use different privacy protecting techniques at different layers of a system. For example, Chiu et al. [19] study privacy requirements for cross-institution image protection and design a system that uses access control rules, RBAC, and watermarking at various levels to offer secure and privacy-aware, cross-institutional image sharing.

Cryptographic approaches to patient privacy. Cryptography is a necessary tool for privacy in eHealth systems [20]. For example, Van der Haak et al. [21] use digital signatures and public-key authentication (for access control) to satisfy legal requirements for cross-institutional exchange of electronic patient records. Ateniese et al. [22] use pseudonyms to preserve patient anonymity, and enable a user to transform statements concerning one of his pseudonyms into statements concerning one of his other pseudonyms (e.g., transforming a prescription for the pseudonym used with his doctor to a prescription for the pseudonym used with the pharmacy). Layouni et al. [23] consider communication between health monitoring equipment at a patient's home and the health-care center. They propose a protocol using wallet-based credentials (a cryptographic primitive) to let patients control when and how much identifying information is revealed by the monitoring equipment. More recently, De Decker et al. [7] propose a health-care system for communication between insurance companies and administrative bodies as well as patients, doctors and pharmacists. Their system relies on various cryptographic primitives to ensure privacy, including zero-knowledge proofs, signed proofs of knowledge (a signature scheme which uses zero-knowledge proofs to sign a message), and bit-commitments. Their system is explained in more detail in Section 5.

2.2 Ensuring doctor privacy

A relatively understudied privacy aspect is that of doctor privacy. Matyáš [5] investigates the problem of enabling analysis of prescription information while ensuring doctor privacy. His approach is to group doctors, and release the data per group, hiding who is in the group. He does not motivate a need for doctor privacy, however. Two primary reasons for doctor privacy have been identified in the literature: (1) (Ateniese et al. [22]) to safeguard doctors against administrators setting specific efficiency metrics on their performance (e.g., requiring the cheapest medicine be used, irrespective of the patient's needs). To address this, Ateniese et al. [6, 22] propose an anyonymous prescription system that uses group signatures for privacy; (2) (De Decker et al. [7]) to prevent a pharmaceutical company from bribing a doctor to prescribe their medicine. De Decker et al. also note that preserving doctor privacy is not sufficient to prevent bribery: pharmacists could act as *go-betweens*, revealing the doctor's identity to the briber. They propose a privacy-preserving health-care scheme that incorporates the roles of pharmacist and health insurer as well as doctor and patient.

2.3 Observations

In the above overview, we observe that current approaches to privacy in eHealth mostly focus on patient privacy and try to solve it as an access control or authentication problem. However, eHealth systems involve many different roles, and these roles have their own privacy concerns. We believe that doctor privacy is as important as patient privacy and should be studied in more depth to avoid situations such as doctor bribery (cf. Section 2.2). In addition, we consider that one party's privacy may depend on another party (e.g., in the case of a pharmacist revealing prescription behaviour of a doctor). Our opinion is that offering privacy is insufficient if privacy can be reduced in such ways.

It is clear from the analysis that privacy in eHealth systems needs to be addressed at different layers: use of cryptography guarantees privacy at the foundation layer; access control ensures privacy at the service layer; privacy by design addresses privacy concerns at the system/architecture layer. Since eHealth systems are complex [24] and rely on correct communications between many sub-systems, we strongly advocate to study privacy in eHealth as a communication problem. In fact, message exchanges in communication protocols may leak information which leads to a privacy breach.

Privacy properties such as anonymity, unlinkability, untraceability etc. have been studied in the literature. All these notions play a role in eHealth systems and each provides a different strength of privacy that can be *enabled*. However, enabling privacy is far from enough. In many cases, a system must *enforce* user privacy instead of allowing the user to pursue it. Enforced privacy has been considered in other domains. Below, we briefly sketch highlights in development of the notion of enforced privacy from other domains.

Enforced privacy in other domains. In the literature, the notion of enforced privacy was studied first in electronic voting. Benaloh and Tuinstra [25] introduce the notion of *receipt-freeness*, which expresses that a voter cannot gain any information to prove to a vote-buyer how she voted. This notion preserves voter-privacy even when a voter actively seeks to renounce that privacy, as in the case of vote-buying. Another, stronger notion of privacy is coercion-resistance [26], stating that a voter cannot cooperate with the intruder to prove how she voted. Both notions of privacy actually capture the essential idea that privacy must be enforced by a system upon its users, instead of merely offering it.

Enforced privacy has been studied outside voting. For instance, a few papers [27, 28] have identified a need for receipt-freeness in online auctions. In eHealth, however, enforced privacy has received to date little attention.

3 Key privacy challenges

Considering how the notion of enforced privacy applies to the eHealth domain leads us to identify two key privacy challenges for the domain:

- *enforced privacy*, e.g., a doctor cannot prove to a pharmaceutical company which medicine he prescribed; and
- *privacy in the presence of others*, e.g., a patient cannot help a doctor to prove he prescribed her medicine.

Satisfying these privacy notions is not easily in any setting. However, the added complexity of the eHealth domain (where a “break-the-glass” requirement exists to ensure emergency access to records) makes these formidable challenges.

3.1 Challenge I: enforced privacy

Enforced privacy plays an important role in eHealth systems, especially for doctors. A typical scenario can be described as follows. A pharmaceutical company seeks to persuade a doctor to favor a certain kind of medicine by bribing or coercing. To prevent this, a doctor should not be able to prove which medicine he is prescribing to this company (in general, to an adversary). This implies that doctor privacy must be enforced by eHealth systems. Generally speaking, a doctor should not be able to prove what he prescribed to any third party except for trusted authorities.

Enforced privacy in eHealth is hardly studied. As such, a proper understanding (beyond the anecdotal scenario given above) of the importance of enforced privacy is absent. Therefore, it is important to investigate which roles in eHealth systems require the notion of enforced privacy. It is also interesting to study which cryptographic techniques can be employed to enforce privacy. Development of systems providing enforced privacy will benefit from privacy-enforcing techniques used in other domains. These include techniques to guarantee receipt-freeness and coercion-resistance, for example chameleon bit commitments as used in a receipt-free online auction protocol [27].

To tackle this challenge, we propose to first focus on lifting formal definitions of enforced privacy to the eHealth domain, and secondly to develop efficient techniques to verify enforced privacy in eHealth. Due to the complexity of eHealth systems, all these remain as scientific challenges.

3.2 Challenge II: privacy in the presence of others

The notion of enforced privacy emerged in voting systems and online auction protocols. In these domains, privacy requirements are mainly focused on the central role (voter and bidder, respectively). In stark contrast, eHealth systems involve many different, non-central roles. Some of these roles have access to sensitive information which reveals something about the privacy of another role. For example, a pharmacist has access to prescriptions, and thus knows something about the prescription behaviour of a doctor. Such a party may be bribed or coerced to help break the other party's privacy. Literature [5, 7, 22] underlines the need to protect a doctor's prescription pattern. This means that no one, except for the doctor himself or trusted third parties, must be able to link the doctor to his prescriptions. In order to obtain a doctor's prescription pattern, an adversary can bribe other parties to reveal their private information which lets the adversary determine a doctor's prescription. This leads us to formulate the requirement of *third-party-independent doctor privacy*: no third party should be able to help the adversary link a doctor to his prescription. On the other hand, these third parties can also help to protect a coerced user. We therefore distinguish two cases:

- *coalition-enforced privacy* (CE-PRIV): a third party helping to protect the coerced user's privacy; and
- *third-party-independent privacy* (TP-INDEP): a third party helping the the adversary to break a user's privacy.

In the first case, the third party cooperates with the coerced user to protect the coerced user's privacy, and reveals his secret information to the coerced user if necessary – forming a coalition, which enables the coerced user to hide from the adversary. For example, a patient cooperates with a bribed doctor to lie about which medicine the doctor prescribed. In the second case, the third party reveals (whether by choice or coercion) his private information to the adversary, enabling the adversary to breach the other user's privacy. For example, a pharmacist can help to breach doctor privacy, by revealing the doctor's prescription behaviour to a pharmaceutical company. In some cases (such as the example), the doctor's privacy is breached without involving the doctor.

We emphasise that TP-INDEP is different from enforced privacy: in enforced privacy, the revealing party breaches her own privacy, while in TP-INDEP, she helps breach another's privacy.

CE-PRIV and TP-INDEP are new notions of privacy, which have not been studied in the literature. In our view, these privacy notions are important for eHealth systems, and stand on their own as privacy challenges.

4 The need for a formal approach

We believe that to solve the two key challenges in a generic fashion, an improved understanding of the concepts *enforced privacy* and *privacy in the presence of others* is necessary. Moreover, we feel that an evaluation method is necessary to validate that a proposed solution indeed addresses these challenges. We argue that neither understanding nor evaluation framework can be properly addressed without formal methods.

In the literature, many research efforts have been devoted to ensure enforced privacy properties for electronic voting. However, despite the best intentions (e.g., [25, 29]), receipts have time and again been found (e.g., [30, 31]). This propose-attack cycle underlines the need for formal methods, which are mathematically based techniques to specify and verify systems.

This is especially pertinent in the eHealth domain, where enforced privacy is a new concept. Moreover, in the eHealth domain, privacy has focused on access control and system design – but even under the assumption of perfect cryptography, communications may reveal private information (cf. the above mentioned attacks). Finding such attacks manually is error-prone, and can give no assurances of completeness. On the other hand, formal verification can give some assurances. Since the eHealth domain stands to benefit so strongly from employing formal methods to express and evaluate security requirements, we fiercely advocate its use.

Current formal approaches to enforced privacy. In voting, several formalisations of enforced privacy properties have been proposed. Delaune et al. [3] develop their formalisation of receipt-freeness and coercion-resistance based on observational equivalences in the applied pi calculus [32]. Automatic verification techniques within the applied pi calculus framework have been proposed by Backes et al. [33]. Their approach focuses on remote electronic voting protocols, and mainly deals with coercion-resistance. Baskar et al. [34] define a language to specify voting protocols and use an epistemic logic to reason about receipt-freeness. Although it is relatively easy to express privacy properties based on logic of knowledge, it is rather difficult to develop verification techniques within such a logical framework. Jonker et al. [35] introduce a formal framework combining knowledge reasoning and trace equivalences to model and reason about receipt-freeness for voting protocols and provided a quantitative definition of voter-controlled privacy. Based on the work of Delaune et al. [3], Dong et al. [4] formalise receipt-freeness in online auction.

The use of process theory has led to success in voting, and the possibility of lifting this to other domains has been shown. However, an eHealth system has a large diversity in roles, something not seen in voting systems or auction systems. As such, a direct applications of formalisms developed elsewhere to eHealth can only approximate the subtleties of (coalition-)enforced privacy in eHealth. It is still a challenge to formally define and verify privacy, enforced privacy, privacy in the presence of other in eHealth.

5 Towards formalising enforced privacy

A case study. Currently, we are investigating[2] privacy of the DLV08 protocol [7]. The protocol involves five main roles: patient, doctor, pharmacist, medical prescription administration (MPA), and insurance company. It works as follows: first, a patient communicates with the doctor to get a prescription. The patient then communicates with the pharmacist to receive the medication prescribed. Next, the pharmacist communicates with the MPA for a refund. The MPA sends an invoice to the patient's insurance company, and once this is paid, the MPA pays the pharmacist.

We model each role's behaviour as a process in applied pi. Thus, the protocol is modelled as the parallelisation of all these processes[3]: $P_{dr} \mid P_{pt} \mid P_{ph} \mid P_{mpa} \mid P_{hii}$. The DLV08 protocol claims (amongst others) doctor-enforced privacy (a doctor cannot prove what he prescribed), and third-party-enforced doctor privacy (third parties cannot help the adversary to reveal the doctor's prescription pattern). To check these claims, we formalise doctor-enforced privacy and third-party-independent doctor privacy as observational equivalences and verify whether DLV08 satisfies either using the automatic verification tool ProVerif [36].

To illustrate how we approach the formalisation, we sketch our formalisation of doctor-enforced privacy. Intuitively, doctor-enforced privacy means that the adversary cannot distinguish between a doctor prescribing a and claiming to have prescribed a, and a doctor prescribing b while claiming to have prescribed a. We model this roughly as $P_{dr}(a, a) \approx {P_{dr}}'(b, a)$, where $\approx$ denotes observational equivalence. Note that the doctor is lying in the second case, thus he behaves differently – hence we do not write $P_{dr}(b, a)$. Naturally, we do not check this in isolation, but in the presence of all other parties, i.e., we verify whether $P_{dr}(a, a) \mid P_{pt} \mid P_{ph} \mid P_{mpa} \mid P_{hii} \approx {P_{dr}}'(b, a) \mid P_{pt} \mid P_{ph} \mid P_{mpa} \mid P_{hii}$.

Future directions. Existing formalisations (in voting) of enforced privacy using observational equivalence [3] provide voters with a fixed defensive strategy. This approach implies that the coerced voter is teamed up with another voter, such that one of their two cast votes matches the adversary's wishes. Privacy is preserved if the adversary cannot determine which of them cast his vote. This forming of defensive coalitions[4] was introduced as a modelling trick to ensure observational equivalence between an execution where a coerced voter complies

[2] For the latest developments, see `http://satoss.uni.lu/projects/epriv/`.

[3] We omit some details, such as multiple instances of processes, here.

[4] Receipt-freeness and coercion-resistance in [3] match our notion of CE-PRIV.

with the coercer and one where she does not. In general, we envisage more applications for coalition-forming in the formal understanding of enforced privacy. On one hand, different parties may form larger coalitions and so have a more robust defensive model. On the other hand, as noted in Challenge II, privacy with respect to an adversary conspiring with multiple parties is inherently lower than the privacy with respect to an adversary without such a coalition or with a smaller coalition. This leads to a variety in behaviour, which is not easily expressed in process theory, but naturally captured in game theory. Hence, game theoretic approaches towards enforced privacy may be promising. In particular, the work of Küsters et al. [37], a game theoretic definition of coercion-resistance in voting, might be adapted towards this end.

Assurance of privacy properties via formal verification is an important step in developing eHealth systems. However, automatic verification of observational equivalences is in general undecidable[5] . Recently, research has been devoted to decision procedures for observational equivalences by focusing on a fragment of the applied pi calculus [38]. It is interesting to investigate the applicability of this research to aid verification of privacy properties in eHealth.

6 Conclusion

eHealth systems are drawing attention because of their potential advantages. However, due to several challenges, the widespread adoption of eHealth systems is still at an early stage. One of the key challenges is to understand privacy issues in eHealth. Current study on this topic mainly focuses on patient privacy and solves it as an access control problem. Privacy issues of other involved parties and during communications are rarely studied so far. We advocated the position that in addition to *enabling* privacy in eHealth (such as protecting patient privacy), *enforcing* privacy plays a critical role, especially for doctors. In addition, we identified another privacy requirement, *privacy in the presence of others*, and argued that a proper understanding requires formalisation, as does genuine verification of these properties. Finally, we sketched our ongoing study of the DLV08 protocol, which claims to enforce privacy for the doctor.

References

1. Meingast, M., Roosta, T., Sastry, S.S.: Security and privacy issues with health care information technology. In: Proc. 28th Annual Conference of the IEEE Engineering in Medicine and Biology Society, IEEE CS (2006) 5453–5458
2. Kotz, D., Avancha, S., Baxi, A.: A privacy framework for mobile health and home-care systems. In: Proc. Workshop on Security and Privacy in Medical and Home-Care Systems, ACM Press (2009) 1–12
3. Delaune, S., Kremer, S., Ryan, M.D.: Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security **17** (2009) 435–487

[5] ProVerif provides limited support for a specific class of protocols.

4. Dong, N., Jonker, H.L., Pang, J.: Analysis of a receipt-free auction protocol in the applied pi calculus. In: Proc. 7th Workshop on Formal Aspects in Security and Trust. Volume 6561 of LNCS., Springer (2011) 223–238
5. Matyáš, V.: Protecting doctors' identity in drug prescription analysis. Health Informatics Journal (1998) 205–209
6. Ateniese, G., de Medeiros, B.: Anonymous e-prescriptions. In: Proc. ACM Workshop on Privacy in the Electronic Society, ACM Press (2002) 19–31
7. De Decker, B., Layouni, M., Vangheluwe, H., Verslype, K.: A privacy-preserving eHealth protocol compliant with the Belgian healthcare system. In: Proc. 5th European Workshop on Public Key Infrastructures, Services and Application. Volume 5057 of LNCS., Springer (2008) 118–133
8. Anderson, R.: A security policy model for clinical information systems. In: Proc. 17th IEEE Symposium on Security and Privacy, IEEE CS (1996) 30–43
9. Louwerse, K.: The electronic patient record; the management of access – case study: Leiden University hospital. International Journal of Medical Informatics **49** (1998) 39–44
10. Reid, J., Cheong, I., Henricksen, M., Smith, J.: A novel use of rBAC to protect privacy in distributed health care information systems. In: Proc. 8th Australian Conference on Information Security and Privacy. Volume 2727 of LNCS., Springer (2003) 403–415
11. Evered, M., Bögeholz, S.: A case study in access control requirements for a health information system. In: Proc. 2nd Australian Information Security Workshop. Volume 32 of Conferences in Research and Practice in Information Technology., Australian Computer Society (2004) 53–61
12. Hung, P.C.K.: Towards a privacy access control model for e-healthcare services. In: Proc. 3rd Annual Conference on Privacy, Security and Trust. (2005)
13. Thomas, R.K., Sandhu, R.S.: Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In: Proc. 11th Conference on Database Security. Volume 113 of IFIP Conference Proceedings., Springer (1997) 166–181
14. Kalam, A., Benferhat, S., Miège, A., Baida, R., Cuppens, F., Saurel, C., Balbiani, P., Deswarte, Y., Trouessin, G.: Organization based access control. In: Proc. 4th IEEE Workshop on Policies for Distributed Systems and Networks, IEEE CS (2003) 120–131
15. Cuppens, F., Cuppens-Boulahia, N., Ghorbel, M.B.: High level conflict management strategies in advanced access control models. Electronic Notes in Theoretical Computer Science **186** (2007) 3–26
16. Sneha, S., Varshney, U.: Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. Decision Support Systems **46** (2009) 606–619
17. Ko, J., Lu, C., Srivastava, M.B., Stankovic, J.A., Terzis, A., Welsh, M.: Wireless sensor networks for healthcare. Proceedings of IEEE **98** (2010) 1947–1960
18. Maglogiannis, I., Kazatzopoulos, L., Delakouridis, C., Hadjiefthymiades, S.: Enabling location privacy and medical data encryption in patient telemonitoring systems. IEEE Transactions on Information Technology in Biomedicine **13** (2009) 946–954
19. Chiu, D.K.W., Hung, P.C.K., Cheng, V.S.Y., Kafeza, E.: Protecting the exchange of medical images in healthcare process integration with web services. In: Proc. 40th Hawaii Conference on Systems Science, IEEE CS (2007) 131–140
20. Biskup, J., Bleumer, G.: Cryptographic protection of health information: cost and benefit. International Journal of Bio-Medical Computing **43** (1996) 61–67

21. van der Haak, M., Wolff, A.C., Brandner, R., Drings, P., Wannenmacher, M., Wetter, T.: Data security and protection in cross-institutional electronic patient records. International Journal of Medical Informatics **70** (2003) 117–130
22. Ateniese, G., Curtmola, R., de Medeiros, B., Davis, D.: Medical information privacy assurance: Cryptographic and system aspects. In: Proc. 3rd Conference on Security in Communication Networks. Volume 2576 of LNCS., Springer (2003) 199–218
23. Layouni, M., Verslype, K., Sandikkaya, M.T., De Decker, B., Vangheluwe, H.: Privacy-preserving telemonitoring for eHealth. In: Proc. 23rd Annual IFIP Working Conference on Data and Applications Security. Volume 5645 of LNCS., Springer (2009) 95–110
24. Tien, J.M., Goldschmidt-Clermont, P.: Healthcare: A complex service system. Journal of Systems Science and Systems Engineering **18** (2009) 257–282
25. Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections (extended abstract). In: Proc. 26th Symposium on Theory of Computing, ACM Press (1994) 544–553
26. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proc. 4th ACM Workshop on Privacy in the Electronic Society, ACM Press (2005) 61–70
27. Abe, M., Suzuki, K.: Receipt-free sealed-bid auction. In: Proc. 5th Conference on Information Security. Volume 2433 of LNCS., Springer (2002) 191–199
28. Chen, X., Lee, B., Kim, K.: Receipt-free electronic auction schemes using homomorphic encryption. In: Proc. 6th Conference on Information Security and Cryptology. Volume 2971 of LNCS., Springer (2003) 259–273
29. Lee, B., Kim, K.: Receipt-free electronic voting through collaboration of voter and honest verifier. In: Proc. Japan-Korea Joint Workshop on Information Security and Cryptology. (2000) 101–108
30. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: Proc. 19th Conference on the Theory and Application of Cryptographic Techniques. Volume 1807 of LNCS., Springer (2000) 539–556
31. Lee, B., Kim, K.: Receipt-free electronic voting with a tamper-resistant randomizer. In: Proc. 4th Conference on Information and Communications Security. Volume 2513 of LNCS., Springer (2002) 389–406
32. Abadi, M., Fournet, C.: Mobile values, new names, and secure communication. In: Proc. 28th Symposium on Principles of Programming Languages, ACM Press (2001) 104–115
33. Backes, M., Hriţcu, C., Maffei, M.: Automated verification of remote electronic voting protocols in the applied pi-calculus. In: Proc. 21st IEEE Computer Security Foundations Symposium, IEEE CS (2008) 195–209
34. Baskar, A., Ramanujam, R., Suresh, S.: Knowledge-based modelling of voting protocols. In: Proc. 11th Conference on Theoretical Aspects of Rationality and Knowledge, ACM Press (2007) 62–71
35. Jonker, H.L., Mauw, S., Pang, J.: A formal framework for quantifying voter-controlled privacy. Journal of Algorithms in Cognition, Informatics and Logic **64** (2009) 89–105
36. Blanchet, B.: An efficient cryptographic protocol verifier based on prolog rules. In: Proc. 14th IEEE Computer Security Foundations Workshop, IEEE CS (2001) 82–96
37. Küsters, R., Truderung, T., Vogt, A.: A game-based definition of coercion-resistance and its applications. In: Proc. 23rd IEEE Computer Security Foundations Symposium, IEEE CS (2010) 122–136
38. Cortier, V., Delaune, S.: A method for proving observational equivalence. In: Proc. 22nd IEEE Computer Security Foundations Symposium, IEEE CS (2009) 266–276