Improving Availability of Emergency Health Information without Sacrificing Patient Privacy

Inger Anne Tøndel

SINTEF ICT, Trondheim, Norway
Inger.A.Tondel@sintef.no

Abstract. To give proper medical treatment, it is important to have access to updated health information on patients. In emergency situations where the treatment is not planned in advance, vital information will seldom be readily available. Smart cards can improve this, but one has to make sure that patient privacy is not sacrificed to improve availability. This paper discusses possible security solutions for an emergency health card, and evaluates to what extent we can assure availability and privacy at the same time.

1 Introduction

Availability of health information and efficient communication between physicians are main concerns within health care. Many cases of medical malpractice could have been avoided if relevant patient information had been available at the right place at the right time. Although medical information has found its ways into electronic patient records (EPRs), these EPRs will often not be available for health personnel not having a pre-established relationship with the patient. The vision of a Universal Patient Record [5, 8] recognizes that patients typically are treated by different types of health personnel in several healthcare organisations. Information on patients is therefore fragmented among different geographical locations, resulting in a need for better communication of all types of patient information [8].

Availability of health information is important in day to day treatment of patients [9], but the main challenges arise in emergency situations where the physicians have no prior relationship with the patient. Several technologies can be used for improving availability of health information in emergency situations, thereby improving patient treatment. One alternative is smart cards [11], which are in many ways ideal for providing emergency information; they are easy to carry and fit well in a wallet. In addition, information is available also in situations where network connections cannot be obtained [1, 6]. The main alternative is the use of centralized servers where such emergency information can be stored [5], but with such a solution, availability of network connections is required. Another alternative to smart cards is ordinary paper cards. This is an easy solution, but provides insufficient security.

Health information is sensitive information, and when handling such information patient privacy needs to be a main concern. Ideally, improving availability of information for legitimate users should not result in laxer security against other parties. This is not a major challenge in systems where the legitimate users are well defined. In

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

emergency treatment situations, however, the legitimate user cannot be known in advance. One does not know when and where the emergency health information will be needed. The picture becomes even more complicated if one considers using the emergency health card internationally.

There exists many types of smart card use within health care today, e.g. to improve authentication and to hold information on patients as well as health personnel. In this paper, the focus will be on an emergency health card [13], and on how to achieve privacy while not reducing availability of information. Other issues regarding the emergency health card will not be addressed. For health information, legislation puts strict requirements on the protection needed. Knowledge of legislation is therefore important to be able to state what level of protection is adequate. Legislation is however not further discussed in this paper. This is mainly due to the complexity of national and international legislation within this area.

The paper starts with looking at smart cards within health care in general. Then the emergency health card is described in more detail, and the privacy issues of this card discussed. Different possible privacy enhancing technologies are described and the adequacy of the different solutions and possible combinations of solutions are discussed.

2 The Use of Smart Cards within Health Care

Smart cards have found their way into health care systems of different countries. Several types of health cards have been developed, storing different types of information related to patients. An electronic health card for people with diabetes in Germany is described in [3]. [15] describes an e-prescription system where patient smart cards play an important part. [7] describes the first phase of the national health insurance smart card project in Taiwan, and [10] describes health card initiatives in Malaysia. These are just examples. [7] refers to health card projects in Belgium, France and Slovenia, among others.

Most health cards today focus on special patient groups and day to day communication, rather than emergency functionality [2]. This is reflected in the security solutions. An example is the smart card used for e-prescription as described in [15] and the health card solution described in [6] where access to health information is controlled by a PIN provided by the patient. As will be discussed in this paper, this is a solution that can cause problems in emergency situations where the patient may be in shock or even unconscious. However, work has also been done to improve emergency care. The US Armed Forces have developed Personal Information Carriers (PICs) that can store medical records of soldiers [4, 14]. In wartime the independence of communication links is a main advantage, but as [4] states, there are disadvantages with the PIC approach; it is a challenge to provide access to appropriate personnel while denying access to the enemy. Solutions to this problem are however not further described.

An example of a civilian project that focuses on emergencies is FieldCare [12]. But, as opposed to the emergency health card discussed in this paper, FieldCare focuses on communication between cooperating personnel after an emergency has taken place. No information on the health status of patients before the emergency is available. There has also been done little work on security in this project. Another initiative is the Pocket

Doctor System proposed in [14]. This initiative recognizes the importance of knowledge of prior medical history when initiating treatment in emergency situations. A solution is presented where the patient carries a smart card, PDA or similar mobile device that is able to communicate via a wireless interface, and thereby can be easily detected. In the Pocket Doctor System there has been done some work on security, ensuring encryption of the wireless link. In addition patients are able to restrict access to some types of information on the device using passwords. This is a solution that will be considered also in this work, despite the limitations of passwords when it comes to emergency situations, as argued above.

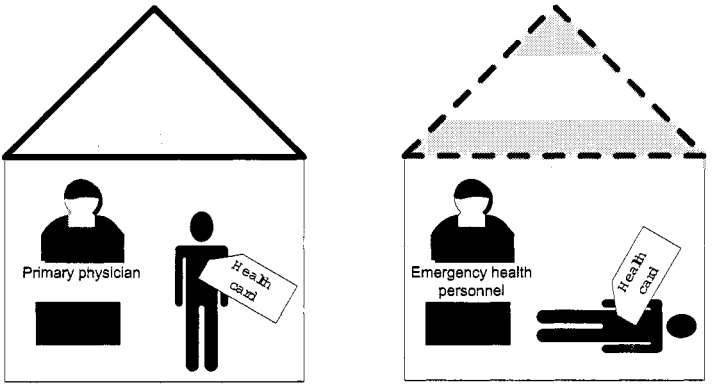
For an emergency health card to be successful, interoperability and wide deployment is of high importance. One approach is to create a reference architecture for smart card based health card applications, as described in [2]. Within the proposed reference architecture it is possible to encrypt and sign information. How such mechanisms can be used in the emergency health card application will be discussed in this paper. Another approach is taken in [1], that describes a web-enabled framework for smart card application. This solution takes into account that smart cards comes with local processing capabilities, and lets the smart cards carry their own record management applet. This ensures that medical information stored on a smart card from hospital A is readable by hospital B. The framework includes a security component that supports authentication and a hierarchical approach to access control, providing different access rights to different types of health professions. However, no details are provided regarding how the access rights of health personnel at a (for the card) unknown organisation is determined.

3 The Emergency Health Card

The emergency health card is not a real application, but an abstract entity that can be used as a basis for discussing privacy vs. availability because of its strict requirements in both respects. The intended use of the application is illustrated in Figure 3. The card will not hold the full medical record of patients, only the core medical information needed in emergency situations. The general health information stored on the card is provided by a physician having knowledge of the patient's health condition. However, the users of the information are mainly health personnel with no previous relationship with the patient. It is possible to write information on the card related to the type of emergency treatment given. This way the patient's primary physician can be updated on the situation at a later stage. Four main types of users have been defined, as described in Table 1.

4 Privacy Issues

Health information is sensitive, and several parties could benefit from getting access to this type of information. Such parties can be insurance companies, possible future employers, journalists (if you are a celebrity) or neighbours and other people you know. With a card solution, you will to some extent be responsible for keeping the health card safe yourself. But since it often will be hard to protect oneself from dedicated robbers, some additional protection is beneficial.



1. The primary physician provides the patient with an emergency health card containing important health information relevant if the patient need emergency health treatment

3. The patient shows the emergency health card to his primary physician after having received treatment from another physician. The primary physician thereby gets to know what treatment has been given and may use this information to further follow up the patient

2. The patient needs some medical treatement, and this treatment is provided by a physician with no previous relationship with the patient. The physician therefore uses the card of the patient to get important information on blood type, allergies, drugs used, etc. to be able to decide on the right treatment. After the treatment has taken place, the physician writes information on the treatment on the card so that this information is available to other physicians at a later stage.

Fig. 1. Illustration of the use of the emergency card application.

Table 1. Description of the different types of users.

User	Description	Access requirements
Card owner	The person that owns the card. Information on the card is related to this person. The owner physically holds the card and is responsible for bringing the card along at all times.	Does not need any access to the information or functionality of the card.
Primary physician	This is the physician chosen by the card owner to be his/her primary physician. This doctor has a special responsibility for the card owner.	Should have access to all information and functionality of the card.
Emergency health personnel	Physicians or other types of health personnel not having a relationship with the card owner. Due to the situation, this person needs information on the card owner to provide proper treatment.	Should have access to emergency health information, and should have access to write information on the emergency treatment given.
Administrative Clerk	A person working at a medical office, responsible for administrative tasks.	Needs access to identification information.

Protection of health information is also important for other reasons. It is in every patient's interest that health information is correct. Erroneous information may result in wrong medical treatment. Erroneous information may also make it hard to prove that medical malpractice has taken place. One may come across unethical doctors that would hide any traces of medical malpractice, or that would like to take opportunities to obtain power over patients. These doctors will have access to the information and functionality of the health card.

5 Possible Solutions

Since protection of the patients' privacy is important, controlling who gets access to the information on the card is a main concern. In addition non-repudiation and integrity are considered important to assure the information on the health card is indeed correct. In the following, different possible solutions to achieve privacy and non-repudiation are discussed.

5.1 Access Control

Enforcing access control will result in some groups not getting access to information. This is the intention of doing access control in the first place, that no one should get access to the information unless they are authorized to get access. However, one must be careful not to shut out legitimate users at the same time. This is especially important in a solution in which a main goal is to enhance availability of information in emergency situations. You will not have time to wait to get access, if you are a legitimate user. If a patient has to choose between correct treatment and increased privacy, chances are high that correct treatment is considered most important. This must be taken into account when considering access restricting solutions.

In this paper, all types of access restricting technologies are considered as access control solutions. This means that authentication solutions and encryption are considered together with more pure access control solutions that come into play after authentication has taken place. Authentication of health personnel in general is however considered out of scope.

Centralized Solutions One possibility is to rely on a central server to enforce access control. This server could, after successful authentication of users, grant access on a per card basis, or to all cards based on knowledge of profession or position of the user. Access could for instance be granted by making the correct encryption key or access token available for the user.

Choosing such a centralized solution results in reduced availability, since access to the card can only be achieved when a network connection and the central server are available. One could also argue that by choosing such a solution, the importance and advantages of the smart card is reduced, since one could fetch the emergency health information on the same server.

An alternative centralized solution is to control access to the card by controlling who gets access to an application needed to use the functionality of the card. Doctors

would then need to authenticate to be able to download the application. The application should be downloaded before an emergency situation takes place, and would only be valid for a limited period. With such a solution, one will not be dependent on network connections to get access to information after the downloading is complete. However, the solution has its drawbacks. Doctors will be required to use time to download and reinstall applications. This task may be seen by doctors as unnecessary, and thereby reduce user-friendliness of the health card system. It may also be hard to control that applications are not distributed to unauthorized users. In addition, this solution has some look and feel of security by obscurity, which seldom inspires confidence.

Another drawback of the application-centred approach is that with this solution it is not possible to give different type of access to primary physicians and emergency health personnel.

Patient Oriented Solutions It is possible to let the patient control access to the card. In this setting this means both providing the physical card to the health personnel, and open the card by providing a PIN or a fingerprint or some other authentication token. In many ways this is an easy and good approach; however one still has to solve what to do if the patient is unconscious or so badly hurt that he/she is not able to make access control decisions. Authentication based on PIN codes will be useless in such situations. Biometrics should work, but doctors may find it uncomfortable stealing for instance fingerprints to get access to information. Another problem with this method is the difficulty of remembering PIN codes that are not often used. Biometrics does not have this problem, but may suffer from false negatives. It is also a more expensive solution. Another consideration is whether it is appropriate to make access control decisions the responsibility of patients maybe being in an awkward situation, possibly psychically unstable.

Card Oriented Solutions One option is to put the main focus on the card, and let the card keep an overview of who has access to what information. This will work well for controlling access to functionality only meant for primary physicians, but the approach fails when it comes to emergency health personnel and administrative clerks. There is no way the card can be able to know in advance the identity of all relevant users of this kind. Having a password or an encryption key known by all users is a possibility, but not very secure. A secret known by all possible users will probably not be a secret for long.

An example of information that only needs to be available to the primary physician is information on emergency treatment given by other physicians. The primary physician is also the only one that should be able to change or delete emergency health information on the card. Access to this information and functionality can be controlled by encrypting the information with the public key of the primary physician, and by knowledge of passwords or other types of secrets.

5.2 Non-Repudiation and Integrity

Using signatures is the common way of stating who is responsible for the information, both in the electronic and paper based world. Signatures are also a natural choice for

achieving non-repudiation of information in this case. Every physician that writes information to the card would then need to sign the information with his or her private key. For other doctors to be able to check the signature later, the certificate of the doctor should be available to all subsequent readers of the information.

Using signatures requires that a PKI is in place. It would also be beneficial to include the relevant certificates on the card, since that would result in the certificates always being available. This may however not be possible due to limited storage capacity on smart cards. Availability of certificates is not as important as availability of emergency health information. It is however worth noting that it will not necessarily be a need for storing many certificates on the card. The primary physician of the card holder will be the one responsible for the information on the card. This physician will probably have written most of the information. In addition physicians providing emergency treatment may write information to the card, but this information will not be present on the card forever, only until it has been read by the primary physician.

5.3 Some Notes about Logging

Logging is a much used mechanism to be able to trace behaviour of users in systems. With the mechanisms discussed up till now, it is possible to trace who has written what information, and that the information has not been altered, but it will not be possible to see who has accessed the information. For health information, access history is of relevance, because privacy is so important. Logs may be used to be able to trace any access to information on the card, but also comes with some challenges. A smart card will not have enough storage to be able to store logs above a very limited size. An alternative is to store the logs on a central server, resulting in the need for available network connections for the mechanism to work. With such an approach, anyone wanting to hide their traces could just disconnect from the network.

One should mark that with normal usage the logs will probably not get that big, if they are transferred to some computer system at the next visit with the primary physician. Storing logs on the card may therefore be rational, since full logs may be taken as a sign of misuse.

6 Discussion

Based on the descriptions of the main alternative security enhancing solutions, it seems that only non-repudiation and integrity can be achieved in a fairly straightforward manner. Privacy is much harder to achieve. No alternative seems to fit perfect for the job, as can be seen in the summary of the solutions in Table 2.

6.1 Possible Combinations of Solutions

None of the privacy enhancing solutions seem to be able to do the job entirely, but combinations of the alternatives may still provide useful solutions. If considering the centralized access control server, this centralized solution can be combined with the patient-centred approach. The centralized access control system could be used if this

Table 2. Comparision of privacy enhancing colutions.

Solution	Drawbacks
Centralized access control server	May reduce availability. High costs due to high availability requirements. May have scaling problems if using the card on international basis.
Centralized application control	Security by obscurity. May be hard to limit availability of the application. May reduce user-friendliness. Cannot distinguish the different user groups.
Patient oriented solution	Patients may be unconscious, or in other ways incapable of making access control decisions. May reduce user-friendliness for both physicians and patients.
Card oriented solutions	Will only work for controlling access for primary physicians.

one is available. If not, the patient may provide access as an alternative. With this combination, the dependence on the availability of the central server is reduced. The dependence on the patient's choices and condition is also reduced; however the problem with unethical doctors and others tricking patients into giving access to information is still relevant. On the other hand, one may ask if this is a real problem since patients may be tricked into revealing the same information verbally without having a card.

The centralized access control server can also be combined with the centralized application control solution. As in the above case, such a solution would use the access control server if available, and grant access based on the availability of an application if not, possibly with reduced access rights. As for the above combination this reduces the problems encountered by the centralized access control server. However, the uncertainty of relying on the presence of an application to prove access rights still applies.

The centralized application control approach can also be combined with the patient-centred or the card-centred approaches. If the patient-centred approach is chosen for combination, health personnel having access to the application may be allowed to access information on the card, but the patient decides the amount of information available. This may be done by providing pin codes to the physician. The patient may now be more certain the doctor is really allowed to access health cards in general. However, the main disadvantages of the patient oriented approach still apply. Combining the centralized application approach with the card-centred solution may be more successful. In this case, primary physicians can access information on the card by using the card-centred approach, while emergency doctors are given access to emergency functionality by virtue of having the application available. This way the main disadvantages of all involved approaches are reduced. One is now able to distinguish between primary physicians and emergency health personnel, and to protect emergency information in general.

As the reader surely has noticed, a few alternatives have been left out in the above discussion. This is due to a judgment of the relevance of the combinations:

- Combining a centralized server with a card-centred approach does not reduce any problems related to emergency operation which is the main problem with availability of the centralized approach.
- Combining a patient-centred and a card-centred solution is not much better than a patient-centred solution since the family doctor of the patient is well known by the patient and not part of the problem when it comes to a patient's access rights enforcement.

One may however combine three or more alternatives. One example of such a solution is to combine one of the centralized solutions with both the card-centred and patient-centred approaches. In such a solution the card will hold information on who is the primary physician, the application or the central access server will hold information on the profession and position of the user, and the card owner will be able to provide access in case the other access control mechanisms fail. But relying on the user to remember passwords that will probably never be used may be optimistic. Biometrics should therefore be used in such a setting.

6.2 Different Protection Requirements for Different Types of Information

An issue that has not been discussed up till now is what type of information will be needed on such a card. Without trying to make a full description of the content, examples of information that can be relevant are name, identification information (for instance photographs) and information on next of kin, religion, blood type, allergies, medications and diagnosis. In addition the card may contain information on emergency treatment given.

The different types of information mentioned above will probably have different needs for protection. Name, identification information and blood type are examples of information that probably could have been printed on the outside of the card without reducing privacy in a great extent. Information on medication and diagnosis may on the other hand be very sensitive.

It is possible to create systems that specify the protection needs of information. Defining protection needs may be the responsibility of the user that writes the information to the card, or it may be specified by the system beforehand, and it may be done at different levels of detail. Because of user-friendliness aspects, it may be advantageous to make the specification of security needs beforehand, and specify the needed security level rather than the actual mechanisms to use, but other solutions are possible.

Assigning security levels to all information on the card makes it possible to give higher protection to the most sensitive information. If combining different access control solutions, one may say that some solutions provide more security than others, and let the type of access control conducted influence the type of information that becomes available to a user. Note however, that it is not only sensitivity that should be considered when assigning security levels to information. The importance of having this information available in an emergency situation is also of high importance.

6.3 What Level of Privacy is "Good Enough"?

The answer to this question will depend on who you're asking. One may say that it should be sufficiently hard to get access to sensitive personal information, but then again, what is "sufficiently hard"? With this emergency health card, the owner of the card will have some responsibility regarding keeping the card safe. How much more is really needed? Is it enough that health personnel need to have a specific application to read the card, or do we need one complex centralized solution that for instance is able to respond to challenges made by the card and provide the answer to the user after he/she has been properly authenticated?

In this emergency health card application, the primary physician shall have access to all functionality and all information on the card. It should therefore be very hard for intruders to get access to functionality only intended for the primary physician. This can be solved with the card-centred approach. Other types of health personnel will have more limited access, though they will probably need access to all or most of the emergency health information. If not, this information need not be put on the card in the first place. Some of this information may be very sensitive, but very important to provide high quality emergency care.

It is hard to provide access only to health personnel involved in patient treatment, since one does not know beforehand who these will be. Maybe part of the access control therefore should lie in the decision on what information to include on the card. This could be a decision made by the primary physician and the patient together. Technically, we can make it harder for intruders to get access to this information, for instance by encoding the information in proprietary ways so that only the correct application can easily read it, or by requiring a valid finger print from the patient; but it will never be foolproof. Dedicated intruders may still be able to get hold of information. However, if we do our job well, it will probably be easier to get to the information by other means.

6.4 How Much is Privacy Worth compared to Cost and User-Friendliness?

Some of the privacy enhancing solutions discussed will reduce user-friendliness or increase implementation costs. Therefore some judgment is needed regarding whether or not the increased privacy is really worth the effort.

Centralized access control servers may prove to be a costly solution, especially because of the strict availability requirements. The costs may be even higher if considering using the card internationally. Biometrics may also be costly to implement, because of all the extra equipment needed.

Reduced user-friendliness will be experienced by the centralized application control solution, since health personnel would need to download the application themselves, especially if this need to be repeated often because of limited validity periods of applications (to increase security). The patient-centred approach also may reduce user-friendliness, both for patients and health personnel. Using passwords that need to be remembered by the patient is particularly hopeless, since these probably will not be remembered in the first place, and will not be available anyway if the patient is unconscious, in shock or similar.

7 Conclusion

The strict availability requirements, and the fact that the users cannot be predicted beforehand, seem to make it impossible to guarantee full patient privacy. However, by being careful with what information to put on such a card, and by combining different solutions, it seems to be possible to achieve adequate protection of information in most cases. More work needs to be done regarding what level of protection is actually needed, and compare this to the cost of solutions, both when it comes to user-friendliness and development and equipment costs. Maybe we will find that we can easily make a solution that will be good enough for most people, while celebrities may feel that they do not get adequate protection. They may compensate for this by physically protecting the card better. However, here again the conflict between availability and privacy comes into play.

Acknowledgments

This paper is based on work done in my Masters thesis at the Norwegian University of Science and Technology (NTNU). I would like to thank Professor Svein J. Knapskog at NTNU and my supervisors Ståle Walderhaug, Per Håkon Meland and Lillian Røstad at SINTEF ICT for helpful feedback during this research.

References

1. Alvin T.S. Chan, Jiannong Cao, Henry Chan, and Gilbert Young. A Web-Enabled Framework for Smart Card Application in Health Services. *Communications of the ACM*, 44(9):77–82, 2001.
2. A. Georgoula, A. Giakoumaki, and D. Koutsouris. A Multi-layered Architecture for the Development of Smart Card-based Healthcare Applications. In *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, volume 2, pages 1378–1381, 2003.
3. G. Gogou, A. Mavromatis, and N. Maglaveras. DIABCARD CCMIS - A Portable and Scalable CPR for Diabetes Care. *IEEE Transactions on Biomedical Engineering*, 49(12):1412–1219, 2002.
4. Dean S. Hartley. Simulating without data. In *Proceedings of the 2002 Winter Simulation Conference*, pages 975–980, 2002.
5. Jagib S. Hooda, Erdogan Dogdu, and Raj Sunderraman. Health Level-7 Compliant Clinical Patient Records System. In *Proceedings of the 2004 ACM symposium on Applied computing*, pages 259–263, 2004.
6. Geylani Kardaas and E. Turhan Tunali. Design and implementation of a smart card based healthcare information system. *Computer methods and programs in biomedicine*, 81:66–78, 2006.
7. Chien-Tsai Liu, Pei-Tun Yang, Yu-Ting Yeh, and Bin-Long Wang. The impacts of smart cards on hospital information systems - An investigation of the first phase of the national health insurance smart card project in Taiwan. *International Journal of Medical Informatics*, 75:173–181, 2006.
8. Michael R. McGuire. *Automation of the Patient Medical Record: Steps Toward a Universal Patient Record.* http://www.uprforum.com/, 2001.

9. Per Håkon Meland, Lillian Røstad, and Inger Anne Tøndel. How to mediate between health information security and patient safety. In *Proceedings of PSAM 8*, 2006. To appear.
10. Jay Mohan and Raja Razali Raja Yaacob. The Malaysian Telehealth Flagship Application: a national approach to health data protection and utilisation and consumer rights. *International Journal of Medical Informatics*, 73:217–227, 2004.
11. Katherine M. Shelfer and J. Drew Procaccino. Smart Card Evolution. *Communications of the ACM*, 45(7):83–88, 2002.
12. I. Svagård, J. Gorman, and B. Haugset. How mobile IT-support and patient tags can improve information flow and patient tracking in prehospital medicine. *Akuttjournalen*, 13(2):120–124, 2005.
13. Inger Anne Tøndel. Personal data carriers. Master's thesis, Norwegian University of Science and Technology, Department of Telematics, 2004.
14. D. K. Vawdrey, E. S. Hall, C. D. Knutson, and J. K. Archibald. A Self-Adapting Healthcare Information Infrastructure Using Mobile Computing Devices. In *5th International Workshop on Enterprise Networking and Computing in Healthcare Industry (Healthcom 2003)*, pages 91–97, 2003.
15. Yanjiang Yang, Xiaoxi Han, Feng Bao, and Robert H. Deng. A Smart-Card-Enabled Privacy Preserving E-Prescription System. In *IEEE Transactions on Information Technology in Biomedicine*, volume 8, pages 47–58, 2004.