The mixed management of patients medical records: responsibility sharing between the patient and the physician

Catherine Quantin, Maniane Fassa, Eric Benzenine, David-Olivier Jaquet-Chiffelle, Gouenou Coatrieux, François André Allaërt

The Mixed Management of Patients' Medical Records: Responsibility Sharing Between the Patient and the Physician

Catherine QUANTIN[a,b], Maniane FASSA[b], Eric BENZENINE[b], David-Olivier JAQUET-CHIFFELLE[c], Gouenou COATRIEUX[d], François-André ALLAERT[b,e]

[a]Inserm, U866, Dijon, F-21000, Univ de Bourgogne, Dijon, F-21000, France
[b]CHRU, Service de Biostatistique et d'Informatique Médicale, Dijon, France
[c]Bern University of Applied Sciences et Université de Lausanne, Suisse
[d]Institut TELECOM ; TELECOM Bretagne ; Unité INSERM 650 LaTIM
[e]Ceren Esc Dijon & Dpt biostat Ecole de Santé Publique Liège Belgique

Abstract: Through this article, we propose a mixed management of patients' medical records, so as to share responsibilities between the patient and the Medical Practitioner by making Patients responsible for the validation of their administrative information, and MPs responsible for the validation of their Patients' medical information. Our proposal can be considered a solution to the main problem faced by patients, health practitioners and the authorities, namely the gathering and updating of administrative and medical data belonging to the patient in order to accurately reconstitute a patient's medical history. This method is based on two processes. The aim of the first process is to provide a patient's administrative data, in order to know where and when the patient received care (name of the health structure or health practitioner, type of care: out patient or inpatient). The aim of the second process is to provide a patient's medical information and to validate it under the accountability of the Medical Practitioner with the help of the patient if needed. During these two processes, the patient's privacy will be ensured through cryptographic hash functions like the Secure Hash Algorithm, which allows pseudonymisation of a patient's identity. The proposed Medical Record Search Engines will be able to retrieve and to provide upon a request formulated by the Medical Practitioner all the available information concerning a patient who has received care in different health structures without divulging the patient's identity. Our method can lead to improved efficiency of personal medical record management under the mixed responsibilities of the patient and the MP.

Keywords: medical record, patient identifier, direct access, data security, privacy, E-health

Introduction

The challenges of gathering and updating patients' administrative and medical data so as to reconstitute patients' medical histories, in order to improve their health care and ensure the success of public health strategies, are being discussed and analysed by

national, European and international health authorities. However, the main problem faced by patients, health practitioners and the authorities is to gather and update the correct administrative and medical data belonging to the right patient, and not anybody else, so as to reconstitute the patient's medical history accurately. Today it is technically possible worldwide to reconstitute almost automatically any patient's health care history if at least three conditions are met:

- The existence of appropriate tools for requests
- Guarantees of the interoperability of patient identification data through health structures and guarantees that the patient's health information relates to the patient [1].
- The possibility of correcting and updating patients' health information.

Thus, the administrative and medical data that have been requested must be validated to avoid errors. The first error type concerns the impossibility to gain access to some patient data due to modifications in identifying information because of a marriage (marital name) or a divorce (own family name), for example. The second error type concerns requests for data that belong to another patient, when there are collisions between the identification data of two different patients, which should be very rare if identifiers have been chosen carefully.

Thus, to avoid ethical problems such as consequences related to providing information that relates to another patient, this validation cannot be provided by the Medical Practitioner (MP) acting alone. Patients can confirm where and when they have benefited from health care. Patients who are in good mental health, can reconstitute, verify and update their administrative information more authentically, accurately, and precisely than anybody else. Of course, patients can seek help from the MP if needed. Furthermore, the MP is the only person who can verify the medical coherence of the requested data. MPs know better than anybody else about the disease and medical information of a patient they have cared for for many years.

This is why we propose to rely on the patient for administrative data and on the MP for medical data. As a consequence, we propose in this article the mixed management of patients' medical records, sharing responsibilities between the patient and the MP by making:

- the patient or the patient's legal representative responsible for the validation and updating of a patient's administrative information
- the MP (with the collaboration of the patient if needed) accountable for the validation and updating of a patient's medical information

Of course, in the case of mental handicap, an emergency or a new MP, through our proposed methodology, we suggest appropriate solutions made possible thanks to the existing medical history, current and former health structures and practitioners and the patient's family members, as shown in some recent studies.

The main objective, of this paper is then to propose a new method to reconstitute, update and provide the correct administrative and medical data belonging to a certain patient through the mixed management of patients' medical records. This will empower patients with regard to the management of their health data by increasing their responsibility [2-3], and increase the accountability of MPs concerning the medical data. The second objective, which is no less important, is to avoid ethical problems resulting from giving a patient access to the data of another patient (mistaking

patients). We aim to correct and update patients' health information, so as to reconstitute the data efficiently with little if any increase in MPs' workload and with maximum authenticity and precision in the patient's medical history.

1. Methods

Patients can be considered key elements in the validation of their first and second names, date of birth, the health structures visited and dates of visits. MPs should also be considered core elements in the processes of medical data validation. It means that patients and MPs should be made responsible for the successful validation of the reconstitution and updating of medical history (administrative and medical information) of the patient. The division of responsibilities between doctors and patients is very timely for decision making [4-10], but has not been extensively investigated regarding the management of patients' medical records.

This proposed methodology relies on two processes:
The first process aims to provide patients' administrative data, in order to know where and when patients have received care (name of the health structure or health practitioner, type of care: outpatient or inpatient).

Patients will be responsible for the validation of this information [11-12]. The first objective of this validation is to obtain the right information for the right patient at any time and anywhere and to be sure that the information concerns only the patient and to avoid providing information on another patient. Secondly, the validation of this information retrieval will provide the patient's medical history. During this validation process, the MP may confer with the patient.

The validation of this administrative information will be the exclusive responsibility of the patient, with the help of the MP if needed.

The main objective of the second process is to provide patients' medical information. The MP will be accountable for the validation of these medical data,, with the help of the patient, if needed. For the validation process to be successful and efficient, it will be useful to take into account the help patients are able to provide in terms of their thorough knowledge of their administrative and medical information. In fact, patients who have all their mental faculties know the history of the care they have received better than anybody else. Patients could regularly update administrative and medical data, for example, once or twice a year depending on the national public health strategies with regard to periodic citizen health check-ups initiated by national health authorities or employers, who offer a minimum package of services for prevention and the follow up of workers regarding transmissible and non-transmissible diseases, for example.

During these two processes, of course, patients' privacy has to be ensured
Patients' privacy is one of the main concerns in the storing, sharing or transmission of personal medical data and it is comprehensively covered by legal acts like the HIPAA in the United States or Directive 95/46/EC in Europe. Many companies including employers Insurers or Banks are very interested in gaining access to such data. Recently, attempts to gain illegal access to such data have been reported in the network. Thus, systems to share medical data through open networks like the Internet

need to prevent access to the identity of the patient. Pseudonymization is one of the solutions that have been suggested for this purpose. It provides a trade-off between patients' privacy requirements and society's needs in order to improve health care systems by linking the patient's identity to a pseudonym from which it is not possible to get back to the patient's identity [13].

Cryptographic hash functions like the Secure Hash Algorithm can be used to reach this goal [14]. However, sharing this pseudonym or code without introducing secrecy in its calculation may lead to specific attacks, in particular when the total number of possible messages that could have been hashed (pre-image) is too small. In this case, the authorized receiver as well as a pirate eavesdropping on the communication could retrieve private information. A pirate, who obtains lists of patients' pseudonyms, by illegal access or simply by listening to the Internet network, may be able to retrieve the real identity of the patients.

The solution we have proposed in [15] of using a medical record search engine procedure, which is illustrated in figure 1 and in the appendix, would counter such risks. In the first step, it encrypts the patient's pseudonym (H(PI)) and the secret key to be used for its decryption and, in the second step, sends them through two different channels. If gaining access to private information becomes more difficult for someone who is spying on the network, such as MRSE intruders, it will be almost as difficult for the MRSE and Aggregator entities involved in information gathering, and which may be tempted to obtain information illegally. Any attackers will face a set of patient pseudonyms without being able to identify those associated with the same patient. In fact, a one-time pseudonym will correspond to each request. This is the main interest of using pseudonyms in our proposal.

1.1. FIRST PROCESS: reconstitution of a patient's history

First step: Pseudonymisation of the patient's identity and generation of several pseudonymous codes.

During a consultation between an MP and a patient, the MP enters all the components of that patient's identification such as his first and last names and his date of birth. Of course, the choice of these components will depend on their availability (exhaustiveness) and their quality.

To optimize the request concerning the patient's data, several identifiers can be generated, based on the different combinations of first names, last names and date of birth of a patient as follows:

- If a patient has two last names such as in the case of a married woman or a child whose parents are divorced, one can create two identifiers (one for each last name).
- It is also possible to do the same for one patient who has two first names (like David Olivier or François André).

Thus, if a patient has, for example, two second names and two first names, the 4 combinations of these names can be used to create 4 identifiers.

This information related to the patient's identity will be rendered anonymous (Figure 1 and appendix), using a robust cryptographic hash function with a specific pad to provide 4 hashed patient identities called $H(PI)_1$, $H(PI)_2$, $H(PI)_3$ and $H(PI)_4$. To

improve patient's privacy, the pad used for hash coding is not the same for each request. A specific pad S is generated by the first Medical Record Search Engine (MRS E 1) and sent to the MP, after being encrypted with the MP public key. The MP can then hash the patient's identifiers with this pad. As a consequence the MP sends not only one pseudonymous identifier per patient but a list of pseudonymous partial identifiers for each patient. The aim of this first step is then to obtain several pseudonymous codes, but, hopefully, always the same ones for a given individual in order to link all of the information concerning any given patient.

Second step: Searching for a patient's administrative data.
The Medical Record Search Engine Procedure [15] is used to provide a patient's administrative data (Figure 1 and appendix).

MRSE1 will send the pad S, once the pad had been encrypted with the health structure public key, to all health structures. Each health structure can then search for administrative information corresponding to these pseudonymous codes (by comparing them with hashed identities of the patients cared for in the structure). All the pseudonymous codes created from the different possible combinations of each possible first name, each possible last name and each possible date of birth are considered.

This administrative information will be sent to the MP, through the aggregator, according to Figure 1.

Third step: validation of a patient's administrative data by the patient
Any patient of sound mind is the only person who can confirm, where, when and for what reasons she/he has consulted for health problems: which health structure? At what time, time, day, month and year.

In case of patients with mental handicap, the MPs will help patients to confirm or not the doubtful administrative information, thanks to their experience with these patients and their diseases.

The doubtful administrative information may relate to:

- a long distance between the patient's residence and the health structure the patient supposedly visited,
- discordance between the type of health care provided by that hospital or clinic and the patient's disease. For example, a health structure that cares only for cancers and the patient's disease which is certainly not cancer!

An automatic check for the coherence of a patient's administrative information can be implemented so as to identify, for example, a patient who received care at the same moment (time, day, month year) in two different health structures. It can also check for the coherence of the distance between the patient residence and that health structure.

The main objective of this automatic check for coherence is not to exclude any information automatically, but to help the MP and the patient to highlight potential errors and correct them if necessary

At the end of this validation, the list of administrative information (pseudonymous codes, dates and health structures) to be conserved is transmitted to MRSE 2.

1.2. SECOND PROCESS: access to relevant medical data for patient care.

First step: searching for a patient's medical data.

The Medical Record Search Engine procedure is used to provide a patient's medical data (Figure 1 and appendix).

Each health structure selected by the first process can then search for medical information corresponding to the pseudonymous codes and the dates also selected by the first process.

This medical information will be sent to the MP, through the aggregator, according to Figure 1.

Second step: validation of patient's medical information by the MP

The MP is accountable for the validation of the medical information, with the close collaboration of the patient.

To validate the information, the MP can also rely on an automatic check for coherence of medical data so as to identify:

- Serious events happening simultaneously with less than two weeks interval between them, for example, myocardial infarction (heart attack), strokes (cerebral vascular accidents), and cancers
- Care in a health structure which does not provide care related to the patient's disease.

These events, situations, and doubtful information which have been identified must be confirmed or not by the MP, always with the close collaboration of the patient.

2. Discussion

Some medical practitioners may complain that this procedure will increase their workload because they will be obliged to read all of the information to detect possibly false or missing information. The burden is not as heavy as they may think for many reasons. First, this enquiry on the patient's past history will not be necessary for all patients and generally the contents of their local records are sufficient to treat the patient. Secondly, few patients (but it should be verified by a survey on a real situation) have been hospitalised in many different hospitals and therefore, the number of different medical records that MPs will have to summarise will more frequently be one or two (or eventually three) rather than ten or twenty. Third, it is important to take into account that this work has to be done in collaboration with the patient, who could provide great help in the management of his own records. For example, concerning the doubloon risk (if the patient was registered with different identities than those requested) and the subsequent risk of losing information, it is easy to ask patients if they have been hospitalised in hospitals other than those that answered the requests and provided information. This doubloon risk is reduced thanks to the use of several combinations of the different possible names of the patient. However, the risk of collision, (the amalgamation of two or more MRs from different patients) is then increased. It is usually easy, except in emergency situations, to ask patients if they have in fact been hospitalised in all the hospitals that provided parts of their medical records. This potential collision error could then be largely avoided during the 1st process. As a consequence, this will avoid providing the MP with medical information regarding another patient, which is very important from an ethical point of view. Moreover, the MP's workload would then be reduced in terms of the number of medical records to be analysed. The situation is less easy if the records provided come from the same hospitals, but here again the patient should be able to confirm, during the 1st process, if

the date of the stay is plausible. During the 2nd process, the MP and the patient could verify that the disease recorded corresponds to the patient. Of course, sometimes the patient is not conscious and cannot answer the questions. This case is not frequent, and we must not build a rule to solve an exceptional problem, and secondly, it is in such a case when the patient cannot give any information that it would be useful to have information on his past history quickly even if it is incomplete or insufficiently precise. Fourth, concerning the amount of gathered data, one may think that it could be useful to reduce this amount in order to make it easier to handle. Therefore, we may imagine adding a selection criteria tool to the basic request as in any kind of search engine. The criteria could concern the selection of a time period, a list of hospitals, a clinical department or event, the pathology about which the medical practitioner requests precise information. However, the information, even when reduced in quantity, will still need to be analysed and reorganized by the practitioner.

To facilitate the MP's work and to limit the duration of the patient's medical visit, the 1st process could also be done by the patient alone before meeting the MP, if the patient agrees and has the skills to do it. The feasibility and the consequences of giving patients direct access to their administrative information or their health care records have to be assessed. It would also be interesting to know the proportion of information patients may delete in their health record if they were able to modify it. One important risk is linked to the fact that some patients will voluntarily erase information they do not want to communicate. It is their right, but in such situations, the resulting medical record cannot be considered reliable and will have no legal value to bring evidence in the case of medical litigation. The main drawback in this case would be the loss of confidence between the patient and the physician, which may be prejudicial to the quality of care. Moreover, would a medical practitioner accept to treat patients on the basis of documents that contain potentially incomplete information? In France, for example, the possibility for the patient to erase or dissimulate some information has been widely discussed, but no consensus was found between health practitioners and patients' associations. Some patients' associations want very sensitive data to be masked so that a patient's medical history will not influence the quality of his or her current care. They consider that patients should have the right to mask sensitive health data (HIV/AIDS, Abortion, Psychiatry….) when they are not necessary to treat the current disease. Their request regarding masking data could then be granted. However, health practitioners do not agree as they think that they need all of the information not only to make the right decision, but also to avoid drug interactions and to take due precautions. Health practitioners consider that, at least, they have to be informed that some information was masked.

Moreover, in France, a patient's medical history, in terms of administrative data (when and where the care was given) is already available to every MP in the private health sector. The 1st process, therefore, has already been implemented, without the risk of losing any information if the patient has received care only in France.

On the other hand, the impact of a patient's collaboration with the MP to identify potential errors in his/her records should also be evaluated. For some diseases, the understanding of the natural history is fundamental [16]. Of course the history taking [17] requires the patient's help. A study concerning patients' access [18] reported that a substantial proportion of patients identified factual errors in their records, but concluded that it was difficult to assess the rate of finding clinically important errors. In this procedure, we have to find a balance between the potential increase in the overall

quality of the information induced by patients' management of data collection from all sources and the risk of altering the accuracy of the data when there is the possibility that some information has been erased.

One peculiar point concerns the contribution of the patient to his medical record. Some people may worry that patients can record incorrect information or deliberately falsify their own data. This situation may happen independently of the management of the medical record, in the daily practice of any kind of medical consultation.

It is an unavoidable aspect of the relationship between the patient and the medical practitioner, which is based on reciprocal trust. In cases of medical litigation, which could be induced by a medical error resulting from an erroneous information, it will be fundamental to identify who recorded the information (traceability and signature) to identify who may be liable. Then the judge will eventually investigate whether these incorrect data were introduced by mistake or deliberately.

Of course, appropriate modifications to our methodology have to be proposed in the case of mental handicap, emergency care or even in the case of a patient meeting a new MP. In the case of mental disabilities, the patient's task could be performed by a trusted party that could be chosen by the patient among family members. When the patient meets a new MP, the main question is to know if the new MP will be able to communicate with the previous one. The answer to this question will depend on the patient's willingness. Of course, further work is needed to define more precisely the limits of patients' responsibilities, taking into account their age, mental faculties and disabilities. In the case of emergency care, family members are not always present to provide help. We can imagine that either the emergency physician can be given access to the medical synthesis previously constituted by the MP or apply the methodology proposed in this paper. In the case of an emergency, a physician could exceptionally be authorized to gain access to all of the data requested, even if the patient has not validated the administrative data as planned in the 1st process. Above all, whatever the amount of lost or false information, the situation (from the point of view of professionals and patients) will be better than the great lack of information we have now. Moreover, one last but by no means minor advantage is that these Medical Record Search Engines using Pseudonymisation of patient's identity will make it possible to retrieve the past histories of all patients without the need to reformat the data and above all without the need to build an additional specific structure. Therefore it could be implemented rapidly at a much lower cost than a central medical record structure.

3. Conclusion

The advantage of our methodology lies in the fact that it gives more responsibility to the patients regarding the management of their personal medical records. Increasing the efficiency of this management under the mixed responsibilities of the patient and the MP can help to provide better health care by two means. First, the MP would obtain more reliable information, which would provide a better basis for decision making and lead to more appropriate treatment. Second, the patient would be more involved in his health care. Moreover, the sharing of these responsibilities would enhance the doctor/patient relationship and hopefully mutual trust.

The disadvantages of our proposition are the possible temptations of patients to erase health information. This has triggered a major debate on ethical and medical aspects which has not yet led to a consensus at either the National or European level.

References

[1] Quantin C, Allaert FA, Fassa M, Avillach P, Fieschi M, Cohen O. Interoperability issues regarding patient identification in Europe. Conf Proc IEEE Eng Med Biol Soc du 23 au 26 août 2007; Lyon; France. 2007;1:6160.

[2] Jones PS, Meleis AI. Health is empowerment. ANS Adv Nurs Sci 1993;15:1-14.

[3] Lau DH. Patient empowerment—a patient-centred approach to improve care. Hong Kong Med J 2002;8(5):372-4.

[4] Visse MA, Teunissen T, Peters A, Widdershoven GA, Abma TA. Dialogue for Air, Air for Dialogue: Towards Shared Responsibilities in COPD. Practice. Health Care Anal 2010 Jan 10. (epub ahead of print).

[5] Lopez JE, Orell M, Morgan L, Warner J. Empowerment in older psychiatric inpatients: development of the empowerment questionnaire for inpatients (EQuIP). Am J Geriatr Psychiatry. 2010 Jan;18(1):21-32.

[6] Baars JE, Markus T, Kuipers EJ, Van der Woude CJ. Patients' Preferences regarding Shared Decision-Making in the Treatment of Inflammatory Bowel Disease: Results from a Patient-Empowerment Study. Digestion. 2010;81(2):113-9.

[7] Gerris J, de Sutter P. Self-operated endovaginal telemonitoring (SOET): a step towards more patient-centred ART? Hum Reprod 2010;25(3):562-8

[8] Larkin GL, Beautrais AL, Spirito A, Kirrane BM, Lippmann MJ, Milzmann DP. Mental health and emergency medicine: a research agenda. Acad Emerg Med 2009;16(11):1110-9.

[9] Burton DA, Blundell N, Jones M, Fraser AG, Elwyn G. Shared decision-making in cardiology: Do patients want it and do doctors provide it? Patient Educ Couns 2009 Nov 27. (epub ahead of print)

[10] Tariman JD, Berry DL, Cochrane B, Doorenbos A, Schepp K. Preferred and actual participation roles during health care decision making in persons with cancer: a systematic review. Ann Oncol 2009 Nov 25. (epub ahead of print)

[11] Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private commentary: Open approaches to electronic patient records commentary: A patient's viewpoint. BMJ 2001;322(7281):283–7.

[12] Røstad L. An Initial Model and a Discussion of Access Control in Patient Controlled Health Records The Third International Conference on Availability, Reliability and Security. IEEE 2008;935-42.

[13] Neubauer T, Riedl B. Improving Patients Privacy with Pseudonymization. In: Andersen SK et al, editors. eHealth Beyond the Horizon – Get IT There. IOS Press; 2008. p. 691-6.

[14] Schneier B. Applied cryptography, 2nd edition. Wiley-India; 2007.

[15] Quantin C, Jaquet-Chiffelle DO, Coatrieux G, Fassa M, Allaert FA. Medical record search engines, using pseudonymised patient identity: an alternative to centralised medical records. In: Collaborative meetings on Health Informatics (CoMHI 2009); IMIA WG4(SiHIS), Hiroshima. 2009. p. 5.

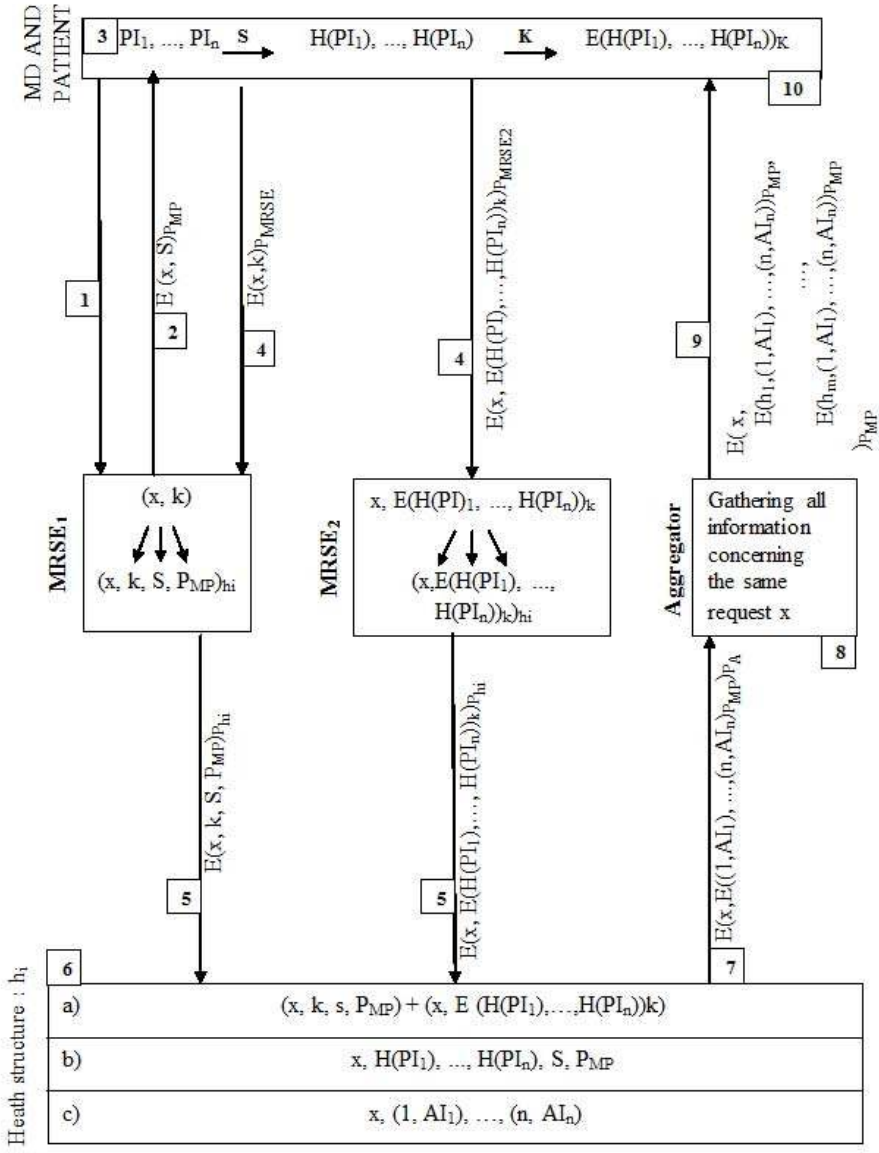
[16] Mehta AB. Anderson-Fabry disease: developments in diagnosis and treatment. Int J Clin Pharmacol Ther 2009;47(Suppl 1):S66-74.

[17] Clauser BE, Balog K, Harik P, Mee J, Kahraman N. A multivariate generalizability analysis of history-taking and physical examination scores from the USMLE step 2 clinical skills examination. Acad Med 200;84(10 Suppl):S86-9.

[18] Ross SE, Lin CT. The Effects of Promoting Patient Access to Medical Records: A Review. J Am Med Inform Assoc 2003;(10):129-38

Legend

Figure 1: Gathering patient's data through Medical Records Search Engines
All cryptographic keys are in index.
All abbreviations are defined in the appendix.



Appendix

It is assumed that participants in these processes know the public keys of the other participants with whom they have to communicate. All data exchanged are encrypted with the receiver's public key before transmission and decrypted with the receiver's private key.

First process:

1) The MP asks MSRE1 for a specific pad.
2) A request number x, and the specific pad S are sent by MSRE1 to the MP
3) Several (n) identifiers are generated using different components of patient identification: PI_1 , … , PI_n
   - Every identifier is hashed using S: $H(PI_1)$, … ,$H(PI_n)$
4) Sending the request to the two MRSEs
   - MRSE1 receives
     a) X, the number of the request
     b) K, a session key
   - MRSE2 receives
     a) X, the number of the request
     b) $E(H(PI_1), \dots ,H(PI_n))_k$, an encrypted list, using K, of hashed identifiers
5) Transmitting the request
   - MRSEs consult a health structure directory
   - MRSE1 sends X, K, S, and P_{MP} the public key of the MP to each of the m health structures
   - MRSE2 sends X, $E(H(PI_1), \dots ,H(PI_n))_k$ to each of the m health structures
6) Inside each health structure hi:
   - $E(H(PI_1), \dots ,H(PI_n))_k$ is decrypted using K
   - The health structure is able to hash (using S) its own database identities and search for administrative information (AI) corresponding to the patient's pseudonyms (comparing its own hashed identities with the patient's hashed identities $H(PI_1)$ … $H(PI_n)$).
   - The health structure generates a list of AI for each identifier sent by the MP: $((1,Ai_1),..,(n,AI_n))$, and encrypts the list with P_{MP}.
7) Transfer of results to the aggregator

   Each health structure sends to the aggregator the number of the request and the list encrypted with the MP's public key: $E((1,Ai_1),..,(n,AI_n))_{P_{MP}}$
8) Gathering all patient information at the aggregator level

   The aggregator collects and gathers together all the information received from all health structures (h_1 … h_m).

   $X, (h_1, E((1,Ai_1),..,(n,AI_n))_{P_{MP}}), \dots , (h_m, E((1,Ai_1),..,(n,AI_n))_{P_{MP}})$
9) These results are sent to the MP
10) The MP will then be able to decrypt these results with is own private key.

The patient can then check and validate the AI corresponding to his/her medical history.

Second process:

The second process relies on the same flow as the first one except that:

- when sending the request, the MP only sends the AI validated by the patient: only the selected health structures with the corresponding selected H(PI) are contacted.
- the results transferred by the health structures to the aggregator and or by the aggregator to the MP include the medical records (MR).