# AN ANONYMOUS HEALTH CARE SYSTEM

MELISSA CHASE AND KRISTIN LAUTER
MICROSOFT RESEARCH

As medical records are converted to electronic form, risks of compromise of patients' privacy increase dramatically. The electronic format makes misuse of many patients' data much easier, so we must be extremely careful with who has access to this data. At the same time, this move to an electronic approach also gives us opportunities to improve patient privacy by leveraging recent cryptographic techniques, and in some ways to improve upon the traditional system.

Here we look in particular at those parties, such as insurers and pharmacies, that are not actively involved in patient care. Currently patients who are insured are required to share the entire record of their medical treatment with their insurer in order to receive benefits, and a pharmacy may store all prescriptions filled for each patient.

However, there is no medical reason for these parties to see this information[1]— they only need enough information to be able to prevent fraud and verify that the provided treatment should be covered under the patient's policy, or that the patient has a valid prescription for the medication being dispensed. We argue that, using recent developments in cryptography, we can allow this verification without revealing any additional information about the patient's record, thus obtaining optimal privacy guarantees.

## 1. High-level description of system:

We envision a system that works as follows:

(1) **Patient sets up an insurance policy with the insurer.** The patient will then receive a token proving that his treatment should be covered according to the given policy.
(2) **Patient visits doctor/hospital.** The patient reveals the relevant part of his policy, and gives the doctor a token for this visit. The doctor/hospital is assumed to be fully trusted by patient with regard to any record or data generated by that visit.
(3) **Doctor bills insurance company.** The doctor generates an anonymous token proving that the insurance claim is valid under the patient's policy and sends it to the insurance company along with a description of the services provided. The insurance company checks this token and reimburses the claim.
(4) **Doctor prescribes medications for patient.** The doctor uses credentials issued by the state that prove his right to prescribe. The doctor will generate a signed prescription, and an anonymous token showing that the insurance will cover the medication, and transfer both to the pharmacy. He will also generate a token for the patient (potentially printed in the form of a barcode).
(5) **Patient goes the pharmacy.** The pharmacy verifies the tokens it received from the patient and the doctor, then issues the appropriate medications.
(6) **Pharmacy bills insurance company.** The pharmacist combines the token from the doctor and the token from the patient and presents the result to the insurance company as proof of the claim. The insurance company verifies it and reimburses the claim.

**Privacy/Security Benefits:** Thus payment for services can be achieved without patient identity being revealed to the insurer or pharmacist and without separate visits by the same patient being linkable.

## 2. Summary of anonymous credential technology

In an anonymous credential system [7, 2, 5], users can obtain credentials from an organization, and then when they want to access a resource/service, generate tokens proving that they hold the necessary credentials. These tokens are anonymous in that they do not reveal any information about the user, they cannot be linked back to the initial issuance, and it is impossible to tell whether two tokens were generated using the same credential. Here we will need anonymous credentials with the following features:

*Basics:* A user receives a credential which contains a set of attributes, and they can issue tokens proving that: (a) they have a given attribute, (b) they do not have a given attribute, (c) they have an attribute within a given range, or (d) any combination of such statements.

*Delegation* [1]*:* A user with a credential from an organization can issue a delegated credential to another party. This party will then be able to prove ownership of a credential that was issued by someone with a valid credential from the organization (without revealing information on this intermediary user). The

[1] We assume that once all information is stored electronically, drug-interaction errors will be caught automatically, and pharmacies will not need to play as large a role in this process.

user can also choose which of its attributes will be included in the delegated credential.

*Single-Use* [3]*:* In some cases it is important to ensure that no credential is used more than once in the same setting. In this case we require that the user generate a single-use token for each setting - if the user generates 2 tokens for the same setting, it will be easily detected, but as long as each use is in a different setting, there will be no way to tell that multiple tokens were generated by the same user.

*Endorsement* [6]*:* We can generate a token in two parts, such that neither is valid without the other. We call these parts the unendorsed token and the endorsement. The endorsement has the feature that it can be made fairly short, regardless of the length of the statement being proven.

## 3. Details of tokens

**Token for patient:** This will be a simple credential including all of the attributes of the policy. (We assume that policies have a standardized form.)

**Token for doctor:** This will be a delegated token with the visit date hardcoded. The patient may also choose to remove some field if it is unrelated to the treatment being performed (e.g. dental credentials may be removed on a visit to the patient's primary care doctor.) Alternatively, the patient could be much more heavily involved, and required to authorize every treatment being claimed.

**Token for insurer:** This is the most complex token. At a minimum, the doctor will use the delegated token to generate a proof that the procedure and/or services claimed are indeed covered, and a single use label for that patient and date (to prevent multiple claims for the same procedure.) If the insurance company's policies are more complex, we might want to allow other features (also achievable with existing techniques):

- Requiring gaps between certain procedures.
- Proving that a preceding procedure has already been reimbursed.
- Proving that the patient's lifetime or annual cap has not been exceeded.
- Proof of signed results from labs for this patient.

**Tokens for the pharmacist:** The doctor will generate an endorsed delegated token for the pharmacy with whatever information is necessary to verify the claim (essentially an endorsed version of the token for the insurer, which reveals only that the prescribing doctor is certified). The unendorsed portion will be sent to the pharmacy, the endorsement will be printed as a barcode and given to the patient.

## 4. Extensions

*Revocation of anonymity/Allowing auditing:* We may want some way to retrieve the full treatment information and identity for each patient, in case of an audit. One option would be to have one (or several) trusted parties who hold (shares of) a decryption key. When a token is formed to be sent to the insurance company, the doctor can also include the encryption under this key of the full treatment information (as well as his signature on this information). If an audit is necessary, then the insurance company can ask the trusted parties to perform the decryption. If fraud is discovered, the doctor can then be held responsible.

*Revocation of policies:* The insurance company may need to revoke policies (e.g. if a patient stops paying premiums). This can be done using existing anonymous credential revocation techniques [4].

*Sharing tokens:* We may want to ensure that a patient cannot share his policy with others. One solution is to assume that all parties (including all patients) have verifiable identities in a public key infrastructure. Another, weaker, approach is to require that a patient share all his rights in order to allow someone else to use his policy. A final approach would be to include the patient name in the policy token that is issued, and in the token the patient shows to the doctor (but not in later tokens). Then the doctor is responsible for verifying the patient's identity.

## 5. Conclusion

We propose an electronic infrastructure which allows insured patients to be treated and their benefits for treatment provided without sharing the information on their medical treatment with the insurer or pharmacy. Our system also allows the insurer and pharmacy to verify the legitimacy of the claims.

## References

[1] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. *Crypto 2009.*

[2] S. Brands. *Rethinking Public Key Infrastructure and Digital Certificates— Building in Privacy.* PhD thesis, 1999.

[3] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. *CCS '06.*

[4] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. *Crypto '02.*

[5] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. *SCN '02.*

[6] J. Camenisch, A. Lysyanskaya, and M. Meyerovich. Endorsed e-cash. *IEEE Security and Privacy '07.*

[7] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, Oct. 1985.