Fine-grained Access Control for e-Health Data

(The official text will be available soon on the UiO web pages)

This thesis will conduct breakthrough research to provide solutions to already identified problems in e-health concerning: dynamic access control and privacy-aware distribution/manipulation of medical data of different granularity and necessity for different requesting health service providers.

Outcomes of the work of the student will include: research papers, together with prototype implementations of the proposed results, as well as recommendation reports for existing state-of-the-art technologies, including comparisons wrt. requirements derived together with partners from the BIGMED project. Testing and usability evaluations of the research results are expected to be done together with partners from the BIGMED project.

An emerging problem for health systems comes from the access control to electronic patient data in the light of the new DNA-based medical information which becomes ever more available. Privacy, consent, and control of who has access to such information are highly important.
A platform for managing DNA-information (like the one developed in the genAP project in Norway) will require a high degree of electronic decision support, customized to various user needs. In addition, different areas of genetic data may be of different degrees of sensitivity (e.g., information on responsiveness to specific drugs may be less sensitive, whereas predictive information on risk of developing neurological diseases may be highly sensitive). We envisage that such DNA-based information will achieve broad dissemination, with applications like personalised medicine. In this context more sophisticated and fine-grained access control requirements appear:

- Access to a specific information most likely will have to be limited to a more precisely defined role of the therapist towards the patient (e.g., the neurologically relevant information may be shielded from a surgeon). Most probably, the patient must also be able to specifically exclude specific persons from access to her records, or parts thereof.
- In some cases, specific consent should be required from the patient (or even from other bodies) before accessing some data (e.g. of predictive nature). This raises the problem of **double authorization** (e.g., only allowing access when the therapist and the patient are jointly asking).
- As different user groups have different needs, information may be presented differently to different user groups (or only accessible at a more superficial level).
- Accountability in the case of DNA-data is more difficult than just logging of access, because when DNA-based information is out it may be to late to “retract it” and the implications of it difficult to quantify. A shocking example here is that the release of the DNA of the parent inevitably breaches the privacy of the children (and other relatives), and current legislation protects privacy only of living persons.

The current electronic patient record systems and other hospital systems are not able to supply access control with a granularity required by the above examples, as well as ensuring accountability more effectively. Moreover, such a system should be flexible enough to cater for new needs of granularity we do not see today. This thesis would try to cater for these by investigating the latest technology of Usage Control, based on mutable attributes and of a continuous nature.

Attribute-based Access Control in Health

Attribute-based Access Control (ABAC) is the successor of Role-based AC where both resources and subjects have attributes, and a set of attributes can be understood as defining a role. ABAC has reached the maturity of OASI standards with XACML 3.0 or SAML 2.0 (including profiles specific for health-care) with existing tools like open-source Balana or PicketBox from RedHat JBoss or proprietary engines like from Axiomatics.

But little adoption can be seen in the Health & Home care IT solutions. If in other industries the role-based approach can be enough, for medical data and processes the ABAC, and more granular extensions of it, are desired due to the highly sensitive and private nature of the information being accessed and the collaborative nature of the work.

Examples: ABAC can handle **non-trivial access policies** like for *collaborative access control,* needed in eHospitals, where multiple subjects should be involved, with varying attributes and roles. A classic example is when the Doctor needs to be present (logged in) in order for the Nurse to perform a procedure. Detailed **auditing of health-care processes** (like administering medicines, preparing operation rooms, home visits) can be done using the notion of obligations in which the decision-point instructs the enforcement-point to first perform some audit/logging actions before granting or denying access.

Possible topic direction: establish a strong ABAC foundation for health data access tested together with BIGMED partners. This would also work towards scaling current care technologies to the more complex access policies identified by BIGMED partners.

Dynamic ABAC

Temporary aspects of access control cannot be handled by ABAC, therefore the recent addition of *dynamic attributes and continuous monitoring* (which was also termed Usage Control [Park&Sandhu 2004, Martinelli et al. 2010]). In a dynamic and changing working environment like home care or emergency hospitals, it is often that one subject needs to take over a process of another. In this case the attributes of the substitute need to be altered temporarily to enable her to perform the respective duty under the same access rights as the person being replaced. But these changes are temporary; e.g., just for one hour, after which the entrance card into the elderly home would no longer work, or viewing the patient record is allowed during an emergency process to the doctor on duty, but after that the access becomes again restricted to only the personal doctor.

Possible topic direction: Investigate how dynamic attributes can enable access decisions to be done automatically, so to allow easy integration with tools like those performing optimization of care processes or the semantic reasoners studied in BIGMED and SIRIUS projects. Bring the existing research to a stage ready to be taken up into practical use cases coming from BIGMED. This work can also look into providing adaptive policies and dynamic access based, e.g., on the health task undertaken, time, or location of the resources and subjects. This would streamline the health-care work processes at no expense to the privacy of the patients.

Query-based Access Control

With increased digitalization of health records and eRegistries (e.g., consider the new DNA banks) and smart homes producing additional environmental data, the health sector enters into the big data era. But in health we cannot grant access to someone for the whole data set, nor for whole records. Instead one often wants to grant access only to those pieces of the data that are needed to provide the respective heath service. Even more, one does not want to allow access to data at all (e.g. do not give away not even a single gene sequence), but only grant rights to use some "queries" on the data.

Then an answer is returned, but not the data, and the health service provider gets what it needs to provide the service, whereas the health records get more confidentiality and privacy protection.

Possible topic direction: contribute to the recent advances in query-based information exchange focusing on developing solutions for providing granular access control to health records. This could interact with researchers on information architectures or on data input formats for optimization engines. This work provides privacy to the patient data while contributing to making more effective and targeted care processes.

Group and Possible collaborations

This thesis will be part of the Institute for Informatics of University of Oslo, and will interact closely with the BIGMED project.

There are various collaboration opportunities:

- with the many partners from BIGMED
- with partners from the various projects going on at UiO
- with other international partners, e.g. with existing collaborators, including from Copenhagen (DK), from Italy, from Chalmers (SE), from USA.

More standard information for PhD announcements, including about research environment, etc.