Secure electronic exchange of pathology reports

Access to patient information is necessary to enable doctors and other health personnel to provide adequate treatment. We will describe a model for electronic exchange of pathology reports between different health enterprises. The solution provides secure and restricted access to health information, while ensuring personal privacy protection. The model can also be used for exchange of information within other specialties.

Roger Bjugn
rogbju@ous-hf.no
Trine Brevig

In order to provide good health care, health personnel need relevant information on the present and previous health condition of the individual patient, including examinations and the results of these. As a consequence of increased mobility in the population, the distribution of functions in the healthcare system and the free choice of hospital, many patients will over time have undergone examinations and treatment in several different health institutions. In a renewed contact with the healthcare system, it cannot be taken for granted that the patient or the healthcare professional will remember or be aware of previous relevant health information.

Most of the recent patient information from the primary health services and the hospitals is found in electronic patient records. In recent years, there has been much debate on the issue of electronic exchange of health information. Viewpoints range from the assertion that «the lack of electronic interaction kills patients» to the view that «privacy regulations are being violated by current IT systems» (1). The Storting has adopted a number of legal amendments that have a bearing on the exchange of health information. It has been decided to establish national consent-based core medical records (2), and in December 2011 the Ministry of Health and Care Services issued a proposal for new regulations regarding inter-enterprise, treatment-oriented health registries in formalised workgroups (3).

Neither consent-based core medical records, nor inter-enterprise health registries in formalised workgroups will on their own ensure that health personnel gain access to relevant health information, or that personal privacy is better protected. To realise explicit political goals, practical solutions must be established to protect people's privacy as well as ensure that health personnel gain access to relevant health information.

We will describe a model for how health personnel can send a request electronically to other healthcare professionals for access to restricted, relevant patient information, without the requester knowing in advance whether or where such information may be available. Exchange of electronic pathology reports across enterprises and health regions is used as an example, but the model is applicable also to other forms of information exchange.

Legal provisions regarding access to health information

The handling of health information in the health and care services is regulated by a number of legal acts and regulations (4). Until recently, the legal framework has been based on the assumption that each individual institution that provides healthcare services maintains an independent health registry. To gain access to health information across organisations, an identifiable person from an identifiable organisation must request such information, and the request must be approved by an identifiable person in the responding organisation.

Health personnel who receive such requests have a general obligation to comply with the request. No information other than what is necessary to provide the patient with adequate health care should be imparted. Patients may refuse information exchange between health personnel, even when the information is necessary to provide health care (5).

Even if the regulations should be amended to allow organisations to establish inter-enterprise treatment-oriented health registries (3), health personnel would still need to request access in the same way as previously, in cases where the information is found in organisations outside the workgroup.

Access to pathology information across enterprises

In Norway, 17 public and two private pathology laboratories examine one million cell and tissue samples each year. When new samples are being diagnosed, it is routine to check whether previous test results are stored in the pathology department's computer system. Often, samples from the patients are available in other pathology laboratories. In some situations, these are therefore contacted to obtain copies of test results or to request material from previously diagnosed samples. The challenge is to find out where such material is located and to gain access to the information when it is needed.

The need for access to relevant patient information from other pathology laboratories is not unique to Norway. In 1999, Denmark established a common online registry (*www.patobank.dk*) for pathology reports (6). For diagnostic work, the pathologists have access to previous test results from all pathology laboratories in the country, without having to request prior permission for such access.

With identical medical needs, but with a legislation which is different from Denmark's, we have modified the Danish model to establish the same functionality for patient treatment within the framework of Norwegian legal regulations.

A model for electronic access to pathology results across enterprises

A solution must comply with prevailing regulations for the handling of patient information (4), and must be adapted to practical routines. The model is based on the following premises:

- A request for access to patient information must be based on a documentable provision of health care to the individual patient.
- Continuous control with regard to the basis of the request.
- Requests and responses concerning the dispensing of pathology results require access control through mechanisms for authentication and authorisation.
- The provision of information should take place through a request to the relevant data controller and continue through active consignment.
- All events regarding requests and consignment of pathology results should be logged.

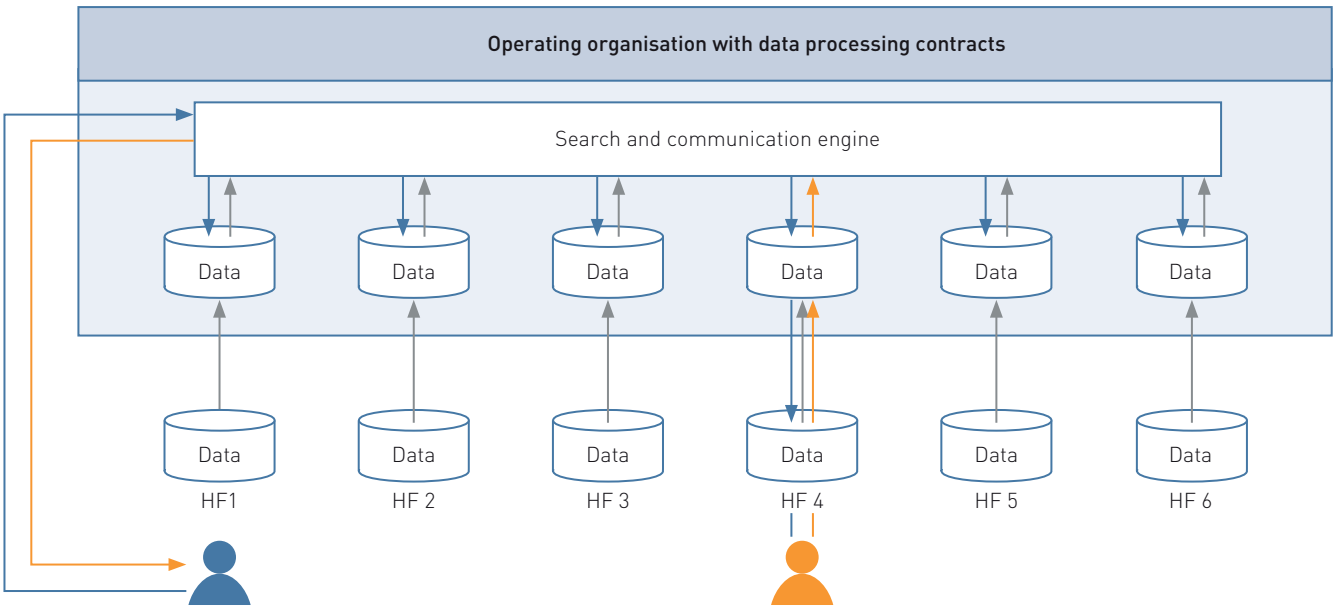

Figure 1: *A model for electronic access to health information (pathology reports) across enterprises. A central operating organisation stores logically partitioned copies of pathology databases from various health enterprises (HF1–6). For diagnostic work, a request for access to patient information can be sent through the Norwegian Health Network to the central operating organisation (marked with a blue arrow on the left side of the figure). The search and communication engine in the central operating organisation will then automatically check whether such information is available in each separate database copy.*

If such information exists, the search engine will send an electronic request to the health enterprise that has such information (HF4 in the figure). Authorised staff members can grant such access, and the information that access has been granted is automatically returned to the operating organisation, which forwards the message to the requesting organisation (marked with yellow arrows in the figure). The diagnostician can then access relevant information in the database copy in the central operating organisation, or download a copy of previous pathology reports as needed. All events regarding requests for and responses to access are stored automatically.

- The organisation that operates the solution should only act as a data processor, and each individual organisation that submits copies of data will act as responsible data controller.
- The patients' right to refuse information exchange between health personnel must be ensured.
- The solution must be practical in use.

Figure 1 illustrates the model, which in our opinion would satisfy these premises as well as the prevailing regulations. The basis of the model is that all pathology laboratories transfer a copy of their patient database to an external operating organisation (regulated by data processing agreements). Copies of pathology results will not be transferred in cases where the patients have refused information exchange. Automatic daily updates through the Norwegian Health Network will ensure that the operating organisation has access to updated information.

In the operating organisation, the copies of the pathology databases are logically partitioned. A request for patient information sent by an identifiable person in an identifiable laboratory will go via the Norwegian Health Network to a search and communication engine in the operating organisation. The engine will search for such information in each individual, logically partitioned database copy. Wherever such information exists, the engine will automatically send a request for access to the electronic work list of the person who has pre-defined authority to respond to such requests.

If the request is granted, information on the identity of the requester and the responder will be automatically stored in the local pathology system, thus complying with the demand for documentation. A message stating that access has been granted is automatically returned to the search and communication engine. The engine will subsequently forward this message to the requesting department. Those who have a defined authority to view such information can then access relevant information in the database copy held by the central operating organisation. Copies of previous test results can be downloaded to the local computer system as needed.

Discussion

The norm for information security in the health, care and social services describes key concepts related to the handling of patient information (4). We will discuss some of these concepts and demonstrate how the model complies with the normative requirements and the premises described.

Provision of health care to individual patients

Provision of health care is the basis for a request for access to patient information. This can be ensured by the requirement that only an «active» pathology report will entail an opportunity for electronic requests for access to patient information from other enterprises. «Active» pathology report means that a pathology department has received a sample, but a final report has not yet been provided. If the need for a reassessment of a previous sample should arise, reports that have been submitted could be reactivated, and a request may then be sent.

Authorisation and authentication

Authorisation involves ascription of the right to read, edit, correct, delete and/or lock health information. Authentication refers to secure identification of an authorised user. Authorisation (with defined roles) is safeguarded through a decision made by the head of the department to grant staff members access to user-defined access levels in the data system used by the pathology laboratory. Authentication associated with the use of the data systems is safeguarded through unique passwords for each individual user (7).

Through management of the rights of the individual staff members, the right to request access to patient information can be delegated locally to the personnel that register new samples. The right to see the information can be restricted to the staff members who have the diagnostic responsibility for the pathology sample in question.

Requests to the relevant data controller
The search and communication engine ensures that requests are sent only to pathology departments (i.e. the organisations acting as the formal data controller) that possess information on the patient involved.

Documentation of events and internal control
The model will ensure that relevant information on requests and the responses to them is stored locally in the individual pathology laboratory and in the central operating organisation. By pre-defining possible discrepancies, such as requests for patient information with no subsequent registration of a pathology report, the central operating organisation may send reports to the individual pathology laboratories for local follow-up.

Data controller versus data processor
The model ensures that each individual pathology laboratory complies with the responsibilities of being a data controller. The central operating organisation is only a data processor within the framework defined by a data processing agreement. Through operation of logically partitioned database copies, but with a shared search and communication engine, the operating organisation does not establish a shared health registry, only an event registry.

Practical use for ongoing diagnostic work
The solution outlined will have one pathology department that requests access, and another pathology department that receives the request. The requesting department can choose to establish general procedures to request access to relevant patient information when new pathology samples are registered. The solution illustrated in Figure 1 ensures that the pathologist or screener who will diagnose the sample possesses relevant information from other enterprises available at the time of making the diagnosis. The workflow will thus not be impeded.

Departments receiving electronic requests for access to patient information may semi-automatise their response routines by establishing two response alternatives (yes/no), where «yes» is the default option. Then, the staff member who has the authority to respond to such requests will only need to push a single button. This routine will be simpler and quicker than current practices, where the laboratory staff must make phone calls to each other to search for information. Moreover, the laboratories will be freed from the need to send copies of pathology reports, since the model gives the requester an opportunity to read and download copies of reports if access is granted.

Transfer value
The model is generic and not restricted to pathology. One could imagine corresponding solutions for radiology and other specialties. Even though the model is intended for a routine where several days pass from the arrival of the sample to final report, it may easily be adapted to situations where there is an immediate need for access to health information. The information security norm describes «emergency access» as a possibility for letting authorised users grant access to themselves without following the normal procedure (4). The requirement is that the reason for this emergency access can be documented, and that each individual case is followed up as a discrepancy. In the model outlined, such emergency access can be ensured electronically around the clock.

The development work for this model was partly funded by the Research Council of Norway through the Høykom programme.

Roger Bjugn (born 1961)
PhD, is a board certified pathologist. He is a Special Adviser at the Department of Research Administration and Biobanking , Oslo University Hospital, and works with issues related to IT. The author has completed the ICMJE form and declares no conflicts of interest.

Trine Brevig
is a board certified pathologist and Senior Consultant at the Department of Pathology and Mohs' surgical team at the Department of Dermatology, Oslo University Hospital. Since 2001, she has been medical IT adviser at the Department of Pathology. She initiated and took part in the establishment of the current shared pathology system at Oslo University Hospital. The author has completed the ICMJE form and declares no conflicts of interest.

References

1. Helmers A-KB. Hør her: Fredrik Syversen vs Bjørn Erik Thon. Sykepleien 2010; 98, nr. 12: 78–9.
2. Etablering av nasjonal kjernejournal. Oslo: Helse- og omsorgsdepartementet, 2011. www.regjeringen.no/nb/dep/hod/dok/hoeringer/hoeringsdok/2011/etablering-av-nasjonal-kjernejournal.html?id=651187 (8.5.2012).
3. Utkast til forskrift om virksomhetsovergripende behandlingsrettede helseregistre i formaliserte arbeidsfellesskap. Oslo: Helse- og omsorgsdepartementet, 2011. www.regjeringen.no/nb/dep/hod/dok/hoeringer/hoeringsdok/2011/horing---utkast-til-forskrift-om-virksom.html?id=667358 (8.5.2012).
4. Norm for informasjonssikkerhet. Helse-, omsorgs- og sosialsektoren. Oslo: Helsedirektoratet, 2010.
5. Rundskriv vedrørende tilgang til og utlevering av opplysninger i elektroniske pasientjournaler (IS-7/2006). Oslo: Sosial- og helsedirektoratet, 2006.
6. Vyberg M, Bjerregaard B, Bak M et al. Patologidatabanken. Dansk Selskab for Patologisk Anatomi og Cytologi. Ugeskr Læger 2005; 167: 1401.
7. Veiledende merknader til helseregisterloven § 13 og forskrift 24. juni nr. 628 om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (helse-informasjonssikkerhetsforskriften). Oslo: Helse- og omsorgsdepartementet, 2012.

Received 27 June 2012, first revision submitted 22 August 2012, approved 19 September 2012. Medical editor: Petter Gjersvik.