

# THE **EMPOWERED** PATIENT AND RESPONSIBILITY FOR THE PROTECTION OF PATIENT INFORMATION

By: Ellen K. Christiansen

## THE EMPOWERED PATIENT

The emergence of the "empowered patient" raises the issue of whether this should influence legislation concerning the responsibility for processing patient information. According to Norwegian legislation, patients are entitled to participate in choosing medical treatment on the basis of information from health personnel. Perhaps patients are also capable of taking part, to a greater extent, in the responsibility for the processing of their health information.

## THE EVOLUTION OF THE PATIENT ROLE DURING RECENT YEARS

The position and role of patients in healthcare services has changed over the years. This applies to the position and role of health personnel as well, as both roles are formed in the interaction between patients and health personnel. The mere existence of Patients' Rights Acts in several countries, including Norway, has contributed to making these changes visible<sup>1</sup>. The Act may even have strengthened the process by giving patients more self-confidence, thus making them more aware of their legal rights. Issues encompassed by the Act include the need for patients' consent to medical care as well as patients' rights to necessary care, to participation and information, to access their own medical records and to protection against the distribution of their medical information.

There are several possible ways to illustrate the new patient role by approaching it through the development of the physician's role. One obvious starting point is the paternalistic doctor of yesterday with his (!) medical journals, to which the patient had no or very limited access. One way to describe the changes that have occurred since then is to imagine the physician's journey from the divine doctor to the confident and informative doctor and recently to the co-operative one, who is more like a consultant or advisor for the patient. A more colourful description originated from the Norwegian Medical Association as early as 1998, when the doctor was referred to as

"the patient's pilot on the great and perilous ocean of [medical] information"<sup>2</sup>. Today, it might be more appropriate to describe the doctor as a partner and facilitator for the patient on a more equal basis.

In more recent descriptions of what is frequently called the empowered patient, he or she has been referred to as "a decision-maker" (Norwegian Federation of Organizations of Disabled People), "a participating decision-maker"<sup>3</sup>, a "more demanding consumer", "the impatient patient" and "partners for providers"<sup>4</sup>. It has also been pointed out that the patients of the future will be entitled to customised healthcare because "one size does not fit all"<sup>5</sup>.

## REGULATIONS CONCERNING CONFIDENTIALITY

The Norwegian Health Personnel Act states: "Health personnel shall prevent others from gaining access to or knowledge of information relating to people's health or medical condition or other personal information that they get to know in their capacity as health personnel" (The Norwegian Health Personnel Act, Section 21)<sup>6</sup>. However, this Act also states that patients can exempt health personnel from their professional secrecy. If patients give their consent, health personnel can communicate defined information about the patient to others. In this case, it is up to the patient to define what is meant by the term "others". They are not necessarily identified people; "others" may refer to one or more people or to "everybody",

for example via newspapers or in a discussion on television. This means that patients, albeit with some exceptions, can to a great extent decide that their health information can be communicated to the general public according to Norwegian health legislation.

When it comes to information security, however, the processing of personal data is not governed by health legislation. The Norwegian legislation in the field<sup>7</sup> is based on the Human Rights Act 1998 (Article 8 of the European Convention on Human Rights), Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>8</sup>. But even though a patient can exempt health personnel from their professional secrecy, the patient's consent does not affect the professional duty of health personnel to ensure confidentiality and the right to privacy according to the legislation governing the

protection of personal information. The security level must be maintained, even if the patient does not care whether others are given access to that particular information or not. The justification for this is that the right to privacy is a fundamental human right that cannot be left to individuals to maintain.

One could ask whether the changing patient role should also influence the division of responsibility for the processing of patient information. Is it conceivable that patients

should have an influence on the security level for the processing of their medical data?

## AN EXAMPLE: USE OF E-MAIL

The use of ordinary unsecured e-mail for transmitting health information by health personnel is illegal according to the Norwegian Data Inspectorate and the Norwegian Board of Health. It is not considered secure enough. E-mails can go astray, it is difficult to explore the true identity of the sender and it is impossible to guarantee that the message is not being altered or read on its way. E-mails encompassing confidential patient information should therefore be rigorously secured and encrypted before they are transmitted. This applies independent of the patient's wishes.

It could be of interest to look further into what the risks are and how patients may be affected if everything goes wrong. The legal situation is that if an e-mail goes astray, it might be considered as a breach of professional secrecy by health personnel according to the health legislation. The same applies to e-mails being read on their way or transmitted to another recipient than intended. This is related to health personnel's duty of confidentiality, which entails not only keeping silent, but also actively preventing others from obtaining access to patient information.

Under certain circumstances, a breach of security measures involves the risk of inflicting damage on someone else. It is possible to imagine that an e-mail from a doctor to a patient could be intentionally altered by someone to harm the patient, even though the risk might be considered small. The same risk applies when recipients falsely pass themselves off as someone else. This could give reasons to ask whether the use of e-mail is consistent with the requirements for responsible conduct among health personnel according to the health legislation.

## PROCESSING OF PATIENT INFORMATION IN THE FUTURE

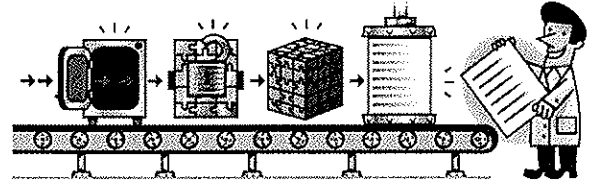
We know that many patients want to communicate with their physicians via e-mail<sup>9</sup>. In the future, this will unquestionably be the case for the use of other electronic means that can help to make life easier for patients, too. There is reason to expect that the use of e-mail will be a matter of course in the years to come.

According to the legislation in force the situation is that, on one hand, patients are deemed competent to exempt health personnel from the duty of professional secrecy. The health legislation presupposes an informed, participating and contributing patient with extensive legal rights to influence the choice of medical treatment. On the other hand, patients have no influence over the security level demanded to protect their health information, whether they themselves consider the information sensitive or not.

Continued on page 25

## Author

*Ellen K. Christiansen*  
Legal adviser  
Norwegian Centre for Telemedicine,  
University Hospital of North Norway  
Ellen.Christiansen@telemed.no  
[www.telemed.no/index.php?cat=4259](http://www.telemed.no/index.php?cat=4259)



## SECURITY SOLUTIONS

### Protect the ordinary PC LAN

The ordinary PC network should be protected through the implementation of an appropriate firewall to protect the LAN from the WAN. However, a firewall isn't sufficient without the proper configuration appropriate to meet the security requirements and the accessibility of the network it is installed on.

### Create a separate radiological LAN

Mission critical devices such as scanners, printers and radiological workstations may be positioned on a network that is physically separated from the network of the ordinary PCs, thus increasing performance and avoiding data sniffing from ordinary PCs. A firewall should control the interaction between the "radiological network" and the ordinary PC network to provide, if needed, accessibility to inner services.

## TELERADIOLOGY ISSUES

Teleradiology systems are much more difficult to protect. As a general rule, any connection to the exterior of the LAN should be encrypted and access should be granted only after proper authentication has occurred.

If there is the need to share the services between the two distant LANs, a Virtual Private Network (VPN) can be established through the creation of an "encrypted tunnel". The most common encryption protocols used in such transmissions are Secure Socket Layer (SSL) or Transport Layer Security (TLS).

## GUIDELINES

In implementing network and information security measures in a radiological network, the following guidelines should be employed:

1. Identify a computer specialist proficient in network security and legal issues;
2. Check the security (physical, behavioural, and network / software issues) with the computer specialist, following established security standards;
3. Define the radiological devices that will be used and the staff who need to access the network (and their corresponding access level);
4. Train people accessing the network on the organisation's standard security procedures; and
5. Plan a periodical security audit and a subsequent activity report.

**Giacomo Luccichenti, MD**  
Staff Neuroradiologist  
Dept of Radiology  
IRCCS Fondazione Santa Lucia  
Rome, Italy  
g.luccichenti@email.it  
www.hsantalucia.it

**Giulio Evangelisti**  
System Security Manager  
Dilogix S.r.l.  
Rome, Italy  
giulio.evangelisti@dilogix.it  
www.dilogix.it

**Stefano Bastianello, MD, PhD**  
Professor of Neuroradiology  
Dept. of Neuroradiology  
University of Pavia – IRCCS  
Fondazione C. Mondino  
Pavia, Italy  
Stefano.bastianello@unipv.it  
www.mondino.it

**Nhan Ngo Dinh**  
Chief Technical Officer  
Dilogix S.r.l.  
Rome, Italy  
nhan.ngodinh@dilogix.it  
www.dilogix.it

**Filippo Cademartini, MD, PhD**  
Staff Radiologist  
Dept. of Radiology  
Azienda Ospedaliero-  
Universitaria di Parma  
Parma, Italy  
filippocademartini@hotmail.com

**Authors**

## THE EMPOWERED PATIENT AND RESPONSIBILITY FOR THE PROTECTION OF PATIENT INFORMATION

Continued from page 23

As long as patients are aware of the risks associated with different security levels for the processing of their health information, it could be asked whether or not they should be allowed to take the responsibility, or at least part of the responsibility, for mishaps that might occur. Is it possible to imagine that the patient and the health service share the responsibility for the processing of the patient's per-

sonal data in the future? Could it be an alternative for the patient to assume the sole responsibility by contract? Another possible future scenario would be the establishing of a double tracked system consisting of one source of information maintained by the health professionals and another managed by the patient herself (himself), such as the patient's own health record, a summary or extract of the patient's health record or a patient's diary managed by the patient.

Empowered patients have undoubtedly come to stay, demanding the right to self-determination. According to this, the interesting discussion is not only how the legislation affects people's behaviour, but also how people's behaviour should affect the legislation in the years to come.