Medical Informatics Europe '97
C. Pappas et al. (Eds.)
IOS Press, 1997

Basic rules for the security of frozen section diagnosis through image transmission between anatomo-pathologists

P. DUSSERRE*, F.-A. ALLAERT**, L. DUSSERRE**
**Centre de Pathologie - 33 rue Bornier - 21000 Dijon France*
*** Service de Biostatistique et informatique medicale du C.H.U. de Dijon B.P. 1542 21034 Dijon France*

Abstract : Telemedicine can provide an alternative solution to the lack of medical resources in areas where the population is no longer dense enough to justify the temporary or permanent presence of certain specialists such as anatomo-pathologists. In the long run certain pre-operational frozen section examinations cannot be carried out without putting the quality of healthcare at stake. The telematic transmission of macro and microscopic images of lesions, under the supervision of a surgeon, to an anatomo-pathologist consultant located off premises allows for the maintenance of equitable care of acceptable quality.

Key words : telemedicine, pathological anatomy, security.

Introduction

Demographic evolution seems to gravitate towards a concentration of the population into urban zones, resulting in a relative desertification of other areas where the density of the inhabitants can no longer guarantee that certain medical specialists will have enough patients to insure their livelihood or that of those who may later replace them.

Telemedicine itself has reached an advanced enough level to fill the gap left by specialists and to maintain an equitable and acceptable access to healthcare by making it possible for patients to be treated from afar.

The biggest difficulties in anatomic pathology could appear in the area of frozen section examinations which require the presence of an anatomo-pathologist who assists the surgeon during the operation. The possibility of transmitting macroscopic and microscopic images of a lesion from a remote place through a telematic line, under the supervision of a surgeon, is a viable alternative to the impossibility of having an anatomic pathologist in person. This technique is therefore referred to as a telediagnosis in anatomic pathology or simply as telepathology. Because these new ways of working (1,2) imply new responsibilities, the systems of security for telepathology, must necessarily be carefully monitored to insure their safety.

After describing the practical aspects of the frozen section examination through image transmission, we will turn to the basic rules needed to guarantee its security.

1. Performing an anatomo-pathological frozen section examination through image transmission

After a review of the pre-operational frozen section examination and its environment, we will consider the role of telediagnosis and its consequences for the patient, the surgeon, the anatomo-pathologist and the healthcare system.

1.1 The pre-operational frozen section examination and its environment

Until recently a patient with a neoplasic lesion was usually operated on in two phases. The

first phase consisted of a simple excision biopsy carried out on the affected tissues and then sent to an anatomic pathology laboratory to determine whether it was benign or malignant. When the tumor was revealed to be cancerous after receiving the analysis results a few days later, the second phase consisted of a possible complementary surgical operation.

Over the years however, the pathologist was called more and more often into the operating room by the surgeon to assist in making decisions about the operation by providing a diagnosis during a so-called anatomic pathology frozen section examination.

Because of the progress made in the various techniques used in the preparation of microscopic slices, the field of accessible organs and their possible diagnosis in frozen section examinations has grown considerably and the method has become of unreputable interest and value. Demands have become such that today pathologists can no longer answer all the needs of the clinics and hospitals in a given region. Moreover the pathologist who used to study a preparation had to diagnose alone and within minutes the appropriateness of the operation. It was impossible to ask a colleague's advice on the spot. If unsure, he had to accept the fact that the diagnosis could not be given immediately. Therefore, the surgeon and the patient had to wait for the laboratory results and, if need be, the opinion of several specialists.

1.2 The role of the telediagnosis in the pre-operational frozen section examination

Progress can be made quickly if telediagnostic achievements are used. In order for this to happen the operating room must be provided with the necessary material for adequate microscopic preparations and an image recording system enabling its numerization and transmission through a healthcare network. With its emitting system, the building is connected to the receptors of the telediagnostic network, which allows for the microscopic examination of the removed tissue.

1.3 The methodology of the frozen section examination through the telematic system

There are two possible situations, depending on the presence or absence of a pathologist in the operating room.

1.3.1 The pathologist is present at the time of the operation

In the case of an uncertain diagnosis, the pathologist, because of the telematic network, can directly communicate the images he is unsure about to a consultant at a more or less remote pathology centre. Undisputably there is an increase in the quality and reliability of the diagnosis.

1.3.2 The pathologist is not present for the operation

If the telediagnosis has been planned, the procedure is the following :

The surgeon needing a confirmation of his diagnosis telephones the pathologist he has planned to contact. They simultaneously watch the same macroscopic and topographic images on their respective screens. The pathologist chooses the problem zones on the screen in collaboration with the surgeon and guides the biopsy. The tissues thus obtained are passed on to a technician trained to manipulate cryostat and to use quick dyes. A series of images are sent to the pathologist who discusses with the surgeon, confirms the diagnosis or offers another. In this manner the surgeon can continue the operation with full knowledge of the nature of the lesion. The tissues are then sent to a laboratory to be examined according to the usual protocol.

When a telediagnosis is needed in unforeseen circumstances this means that the surgeon has to face an emergency that he cannot identify. He uses the network to contact an available

pathologist and, from a distance, the latter participates through telediagnosis according to the previous modality applications.

2. The security of the anatomic-pathology frozen section examination through the telematic system

For hospitals and clinics that do not have a pathologist present, the frozen section examination through telediagnosis is of utmost value provided that its security can be guaranteed. The three main functions of security - confidentiality, integrity, and availability of information - must be insured at the time that the frozen section diagnosis by telematics is taking place.

2.1 The confidentiality of the frozen section examinations through a telematic system

According to the different standardization organizations, the definition of confidentiality is *the property which assures that only authorized users, in normal conditions can have access to the system.* Consequently, this protects the private lives of those individuals who are subject to give their personal details for automatised treatment.

In a system of tele-expertise, there are numerous possibilities for the violation of confidentiality. This can be in the form of theft (of all or part of the system), manipulation errors, whereby information is sent to people not meant to receive it, unauthorized access, falsifying the user's identity, making unauthorized file copies, intercepting messages, etc. All of these possibilities underline the need for physical and computerized protection of the system.

Physical protection requires that a computer system be placed in a protected zone, ideally in a closed room equipped with anti-intrusion detectors. This zone must have a sealed door and have a lock and a digital style electronic alarm system or a micro-processed card reader. For daily use all of the security elements are rarely found together especially when information systems are located in open structures such as medical services where many people circulate. The basic precaution needed to avoid material theft, simple and effective in most cases, is to attach these systems to their bases.

Computerized security entails the protection of the system through passwords or the much more effective micro-processed card reading mechanism for health professionals. The latter process will soon be widely available in private and public hospitals. It will allow the doctor to identify and authenticate himself as such and to name his diagnostic conclusions. Other complementary devices can be recommended such as the automatic stop which is set off as soon as the system is no longer being used after 1 or 2 minutes. It is then necessary for the user to identify himself in order to restart it. A large number of breaches of confidentiality happen on systems which are left to function without surveillance through thoughtlessness or negligence. As concerns the network, the installation of anti-intrusion devices of the firewall kind also protects against the risks of distant « *hacking* ».

Whatever the relevance and power of technical solutions used to protect information, they are ineffective if not accompanied by serious efforts to make the staff aware of the importance of respecting confidentiality. They must be warned of the risks and heavy fines which threaten those who contribute, directly or indirectly, voluntarily, or involuntarily, to the disclosure of registered medical information.

It is, unfortunately, the staff users of the information system who is both in charge of its maintenance and protection, and the ones who are usually the source of problems. Careless talk, the loan or loss of an access card and its personal code, or simple laxness about security rules can be considered as serious offences in light of their possible consequences. The members of

staff, however, can only be held responsible if they were warned beforehand of their duties in this area, but this is rarely the case. Such information should be considered the object of oral and written explanations at the interviewing stage for the job. To materialize the solemn commitment of the staff towards the ethical code and of medical information rights, a contract could be written up and signed by the future employee.

2.2 The integrity of a system of frozen section examinations through a telematic system

Integrity is the quality which insures that information is only modified by its habitual users in normally provided circumstances.

Checking computer entries requires not only allowing entry rights based on one's identification and authentification, but also a signature for any modification of pre-existing information or of any supplementary data. In a tele-expertise transaction, all clinical information and images sent for advice must in the future be signed electronically through the use of a personal card for health professionals so that the doctor who asked for advice cannot deny his interaction with the doctor referred to in the face of a legal conflict. The latter must also sign his response. To supplement this and avoid all lawsuits for delayed answers or the reception of several confusing responses which could interfere with the process, all messages should include the date and time they were sent. All the features of the tele-expertise transaction - clinical data, images, answers given, dates and times - will then be electronically secured into the computer and recorded on a non-erasable recording device so that they cannot be modified. In the case of a lawsuit this can serve as possible proof. The solution would be to have a trusted third party certifying all transactions. However, on a daily basis, their number and volume are so great that it would be a major task to undertake.

Dealing with all the data which the transmission of images and information requires, also creates opportunities for the breach of integrity. The consequences of these violations depend both on their importance and on the field of study they take place in ; the technical solutions should be adapted depending on how tolerable the violation is. A few missing data bits only slightly alter the transmitted image quality whereas it can fundamentally change the meaning of the numbered results.

When there are no acceptable alterations, cryptographic functions can be an efficient monitor. When the information is sent out, all of it is transformed into a given value by a mathematical algorithm. The same algorithm is applied to the information received. The slightest variation between the information sent and that received creates substantial differences in the numbered results before and after transmission. For this reason it is easy to detect. A more classic method would consist of sending out several pieces of information and checking the equivalence of each piece received. The major problem with this method is that it is time consuming and just as sensitive as the cryptage technique. On the other hand, it allows for the identification of altered information with precision.

Because of the possible alterations to transmitted data, all frozen section examinations put through the telematic system must be validated before being used in order to judge if a possible breach of integrity of information can have an effect on the quality of the service provided. For anatomic-pathologists, a validation of the RESINTEL system took place between Boston and Dijon to show that the diagnosis given from glass slides or transmitted images were the same and that changes due to the transferring process did not affect their intrinsic qualities.

2.3 The availability of a frozen section examination through a telematic system

Availability is the skill of an information system to be used by authorized users in normally

provided conditions of access.

An information system's unavailability results either in major breaches of its integrity as concerns its data, application program or materials or a lack of technical and human organisation needed for it to function properly.

The organisation of a system of frozen section examinations through telematics cannot be limited to the installment of a work station linked to a telecommunication network. The medical, paramedical, and technical staff must be prepared to insure the availability of the proposed services. The surgeon asking for advice expects the response of an expert with the necessary qualifications and experience.

Before setting up such a system, serious thought needs to go into putting all the operating conditions into place, making sure that it will be run efficiently and that it is sound in order to insure the system's continuity.

3. Conclusion

Putting a system of anatomic pathology frozen section diagnosis in place through the transmission of images does not only involve laboratory equipment and operation rooms with stations that transmit and receive anatomic pathology images. It also requires a technical environment and administrative organisation which insures its running order in conditions that guarantee confidentiality of exchanged data, their integrity and the continuity of services in the given period. If there is harm done to a patient because of laxness towards these security rules, the hospital and its doctors would be held responsible.

From the start, telediagnosis must be conceived as an alternative solution to a lack of medical resources when taking into account the constraints which result from this and not as a method used when worst comes to worst and which can be more or less improvised.

References

[1] L.Dusserre, F.A. Allaërt, Is telemedicine legal and ethical ? Information and health. Medical information. Legal ethical aspects and public health. "SpringerVerlag", 1996, nb 8, 67-1-6.

[2] L. Dusserre, Legal and ethical aspects of telediagnosis in medicine. Bull. "Ordre des Médecins", nb 6, 1993.

[3] F.A Allaërt, L. Dusserre, Making information systems secure. "Médecins des Hôpitaux ", 1994, nb 41,11-14.

[4] Allaërt F.A., Genestar 0. Physical security of computer systems. Gestions Hospitalières, 1994, nb 339, 646-648.

[5] F. A. Allaërt, D. Weinberg, P. Dusserre, P. J. Yvon, L. Dusserre, Evaluation of a telepathology system between Boston (USA) and Dijon (France) - Glass slides versus telediagnostic TV Monitor. Nineteenth annual symposium on computer applications in medical care. JAMIA. Proceedings SCAMC, 596-600.

[6] F. A. Allaërt, L. Dusserre, Telemedicine and responsibility. Arch. Anat. Cytol. Path. 1995, 4, 200-205.