datenschutz nord

e-pacs Evaluation
Short Public Report

1. Date and time of evaluation

February 5th –August, 29th 2008.

2. Vendor/producer of the IT-product or the provider of the IT-service

Name (company):	Telepaxx Software GmbH
Address:	Wasserrunzel 5, 91186 Büchenbach, Germany
Contact person:	Andreas Dobler

3. Address of the experts

Technical Pilot Expert:	Dr. Uwe Schläger
Legal Pilot Expert:	Irene Karper LL.M.Eur.
Company:	datenschutz nord GmbH
Address:	Barkhausenstraße 2, 27568 Bremerhaven, Germany
phone:	+49(0)471300110
Email:	office@datenschutz-nord.de
web:	www.datenschutz-nord.de

4. Name of the IT-product or IT-service

e-pacs Vers. 3.0

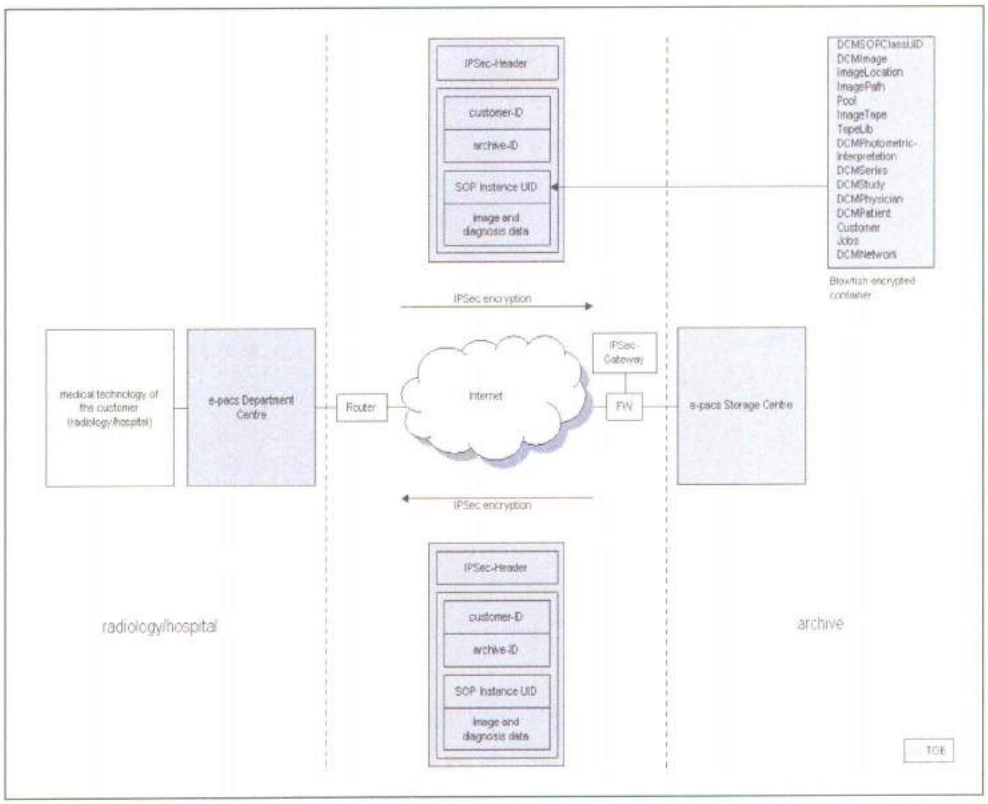
5. General description of the IT-product or IT-service

E-pacs is a central digital image data archive used by radiologists, hospitals and doctors in private practice. E-pacs archives x-rays and other patient-related medical data. It largely comprises two components that are target of this evaluation (TOE); the local e-pacs department server at the customer site and a dedicated external e-pacs deep storage server. The encrypted data are transmitted between these components over an existing network infrastructure.

The e-pacs department server is installed at the radiologist's workplace/at the hospital and allows customers access to the e-pacs storage service. The department server provides the consulting doctor with access to radiological image data for local processing over the respective modules/workstations. The DICOM (Digital Imaging and Communications in Medicine) standard forms the interface between the department server and medical technology, allowing the incorporation of the very latest state-of-the-art radiological equipment. The e-pacs department server also executes data encryption, priority management, transport monitoring and transaction security for communication with the deep storage server in the external DTP centre.

The deep storage server undertakes all customer-related archiving and the actual back-up/recovery and is operated by Telepaxx Software GmbH. This external archive offers all customers a dedicated data management solution, comprising their own database and their own data carrier pool. Incoming data are automatically assigned to the correct customer. Access to the archived data is possible around the clock by means of an automated mass storage system.

The data flow can be described as follows:



6. Targeted countries

The e-pacs storage service is offered to customers with businesses in Germany, as well as internationally. The archive data are archived centrally on servers in Germany.

7. Tools being used by the manufacture of the product

Borland Delphi 4.0

Mircosoft C++ Visual Studio 6.0

8. EuroPriSe Catalogue Version

EuroPriSe Catalogue 0.2

9. Evaluation results

TOE concerning the e-pacs product are the local department server at the customer site and a dedicated external storage server at the archivist site. IT-security in the premises of the controller is not target but side scene of this evaluation,

guaranteeing the protection of relevant data. Within the data flow of e-pacs two major data types can be identified:

Primary data: Medical data (image and diagnosis data)

Secondary data: Header information (customer data) and log data at application level.

Of key importance is the processing of medical data, such as x-ray data or the SOP Instance UID, a categorisation of DICOM, uniquely assigned to each x-ray. In the case of screenings and sonographies, or even in the case of some nuclear-medical images, image data contain additional information on patient names. Under Article 8, paragraph 1 of Directive 95/46/EC, these data are to be categorised as sensitive data and are subject to special regulations.

Furthermore, data on the respective medical practice/hospital department are processed in the header information. The medical data records are archived on the database system for the respective doctor using a consecutive registration number (Archive ID) and a customer number. In contrast to medical data, these data are not stored encrypted at application level. This is due to the fact that the storage server contains log data that serve the management and auditability of the archive.

Except for processing customer data, Telepaxx Software GmbH is the agent of data processing; the customer is the principal in the sense of Article 2 d) of Directive 95/46/EC. Security goals and data protection concept are detailed e.g. in a security policy or a data protection concept and are binding part of the licence and form agreements.

It has to be stressed, that the relevant personal data are pseudonymous. Customer and archive IDs represent pseudonyms that, without additional knowledge, do not enable any further inferences to be made with regard to customers or patients. The additional knowledge required for re-identification is contained in the respective tables on the department server/storage service. Customer ID and customer are assigned on both the department server and the storage server; archive ID and patient are assigned solely on the department server. The pseudonym archiving fully satisfies the principle of data economy and data reduction.

While processing pseudonymous data, members of the Telepaxx Software GmbH have no access to personal medical data. The risks at stake for the individuals with regard to the processing of such indirectly identifiable information are low, so that the application of rules will justifiably be more flexible than if information on directly identifiable individuals were processed.

The storage of medical data is covered by Article 8 para 3 of Directive 95/46/EC as an exception of the basic principle of prohibition of processing special categories of personal data stated in Article 8 para 1 of the Directive: The storage within the e-pacs system is required for medical purposes such as diagnosis of radiologic data or for care and treatment of the health-care service in a particular running case. Responsible for the processing of such data is the customer (i.e. hospital or doctor) as the principal whereas the Telepaxx Software GmbH is the agent, responsible for the technical circumstances of storage. Therefore, members of the Telepaxx Software

GmbH are "another person" in the sense of Article 8 para 3 of the Directive. All employees of Telepaxx Software GmbH are subject to an obligation of secrecy.

As well but subsidiary, the data processing falls under the contractual relationship as laid down in Article 7, b) of Directive 95/46/EC. The doctor is subject to a professional obligation to archive medical data. While this is not uniformly regulated within the member states of the EU, it corresponds to a general legal principle that is laid down in various versions within domestic law (in Germany e.g. within the X-Ray Ordinance). Article 7, c) and can therefore be referred to as a legal principle for archiving. Furthermore, the archiving of medical data – depending on the treatment and state of health – can serve the vital interests of the patient, for example, when access to older image data is required due to a life-threatening situation. Archiving is also based on Article 7, d) of this Directive.

But in the foreground is the preservation of doctor/patient confidentiality, which represents one of the oldest known data protection provisions[1]. This principle is a national legal principle, which is recognised in the legal systems of EU member states in different forms (e.g., in Germany, it falls under the professional standards for doctors and legal sanctions as laid down in § 203 of the Criminal Code) and which protects patient confidentiality against unauthorised disclosure.

Technical/organisational security measures are particularly relevant with regard to the protection of patient confidentiality in the case of the e-pacs storage service. It must therefore be ensured within the framework of archiving by e-pacs that doctor/patient confidentiality is not violated. The admissibility of processing data by a processor does not automatically grant authorisation to disclose medical data to personnel of the data processor. While system administrators who are also employees of a hospital or a medical practice are so-called vicarious agents of the doctor, this does not apply to external specialists. It therefore follows that the disclosure of patient data to medical EDP personnel is permitted. Medical data must never be disclosed to external employees.

The latter is prevented within the framework of the e-pacs archiving service due to the fact that the data are encrypted prior to transmission from the treating doctor to the archivist and are only decrypted by the doctor again after transmission back to the department server. As the treating doctor is the only person who has access to the eToken required for the decryption and encryption of data, no patient data are disclosed to external employees outside the medical practice/hospital during the archiving process using e-pacs. It therefore follows that archivist employees do not have access to archived data, either on the department server, or on the storage server. The fact that doctors working in a group practice each have their own department server and their own key for archiving, ensures preservation of doctor/patient confidentiality as far as other doctors not involved in the respective treatment are concerned.

1 Going back to the Hippocratic oath, approx. 400 BC: "Whatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I shall not divulge, as reckoning that all such should be kept secret".

The protection of patient data is also closely connected with the principle of objects not subject to seizure. It protects the confidentiality between the doctor, who is entitled to refuse to give evidence, and the data subject. Objects not subject to seizure and the doctor's right to refuse to give evidence are key principles which, although not consistently regulated within the EU, must be recognised as general legal principles and are specifically regulated by law in many legal systems. In Germany, this principle is laid down in § 97 of the Code of Criminal Procedure, which will be cited for the purpose of this evaluation. The law governing objects not subject to seizure does not therefore refer solely to objects in the safekeeping of those entitled to refuse to give evidence, but also to patient data in the safekeeping of an external service provider/contract data processor.

The data being handled by the e-pacs storage service are therefore also subject to the regulations governing objects not subject to seizure if they are physically in the rooms of Telepaxx Software GmbH. The requirements on the law governing objects not subject to seizure are optimally implemented in the e-pacs storage centre through the regulations concerning encryption and pseudonyms. These ensure that the encrypted data, if seized by the criminal prosecution authorities, cannot be interpreted by criminal prosecutors on their owns and thus remain fully protected against unauthorised attention. For access to these data, the Crown Prosecution Service requires the specific eToken of the medical practice/hospital.

The security of e-pacs is not only ensured by mechanisms that are an integral part of the actual product, but also assumes a secure application environment. This includes IPSec encryption, a CA server for the generation of IPSec certificates, firewall functionality and a hardware token for the storage of a key with which the archive data are encrypted. The security measures implemented in e-pacs, together with a secure application environment, ensure the authenticity, integrity and confidentiality of both medical data (primary data) and header information/log data (secondary data). The e-pacs product goes above and beyond the requirements, as the technical solutions used enable innovative implementation of the statutory provisions. This particularly applies to the hardware-based encryption mechanism at application level and the use of pseudonyms.

10. Critical Functionalities

None.

11. Privacy Enhancing Functionalities

A key feature of the e-pacs product is that, throughout the archiving process, starting with the transmission form the department server to the storage server through to transmission back to the doctor, the medical data are encrypted and cannot be accessed by the archivist. This type of application-orientated encryption is the data protection measure that covers the most security requirements. Not only are the medical data securely transmitted and archived, the product also complies with the statutory provisions regarding objects not subject to seizure and encryption further ensures the integrity and authenticity of all data.

The use of pseudonyms in the header information also renders it impossible for any inferences to be made regarding individual patients or customers. Thus, header information with pseudonyms ensures the security/confidentiality of all secondary data.

The requirements as stated in the EuroPriSe catalogue are fulfilled. Overall, measures of data protection taken by the e-pacs system are exemplary.

12. Certification of experts

I certify herewith, that the above-named IT-product/IT-service is compliant with the data protection and data security. The detailed analysis is attached.

Bremerhaven, 2008-08-29

Signature of experts:

Dr. Uwe Schläger

Director datenschutz nord Ltd

Irene Karper LL.M.Eur.

Legal Council