Bottlenecks & challenges and RTD responses for legal, social, ethical, and economic aspects of healthgrids : roadmap : V 4.0

STROETMANN, V.; STROETMANN, K.; DOBREV, A.; VAN DOOSSELAERE, C.; WILSON, P.; Andoulsi, Isabelle; Herveg, Jean

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

SHARE

BOTTLENECKS & CHALLENGES AND RTD RESPONSES FOR LEGAL, ETHICAL, SOCIAL, AND ECONOMIC ASPECTS OF HEALTHGRIDS – ROADMAP I

Document ID:	**SHARE-D4.2-revised-v4.0.doc**
Date:	**06/07/07**
Authors:	**I. Andoulsi, J. Herveg, V. Stroetmann, K. Stroetmann, A. Dobrev, C. Van Doosselaere, P. Wilson**
Activity:	**WP4: Ethical, Legal and Socio-Economic Aspects of healthgrids – Roadmap I**
Document status:	**Revised V4.0**
Document link:	**http://eu-share.org/deliverables.html**
Confidentiality:	**Public**
Keywords:	**healthgrid, Legal, Ethical, Social, Economic, Bottlenecks & Challenges**

Abstract: This document provides first insights towards a comprehensive roadmap for ethical, legal and socio-economic (ELSE) aspects of facilitating the uptake of healthgrids in Europe. The roadmap is to be further developed by the end of the project. Based on a storyline model approach, relevant ELSE issues identified are discussed in detail and some generic recommendations are provided.

Document Log

Issue	Date	Comment	Author
0.1	05/02/2007	healthgrid story	P. Wilson
1.1	08/02/2007	First draft roadmap	V. Stroetmann
1.2	08/02/2007	Story contribution	A. Dobrev
1.3	10/02/2007	Economic issues healthgrid story	A. Dobrev
1.4	10/02/2007	Generic approach	V. Stroetmann
1.5	10/02/2007	Quality review, roadmapping approach & socio-economic issues	K. Stroetmann
1.6	10/02/2007	Quality review, social issues	S. Robinson
1.7	11/02/2007	Legal issues healthgrid story	I. Andoulsi
1.8	11/02/2007	Legal issues healthgrid story	P. Wilson
1.9	12/02/2007	Review	V. Stroetmann
1.10	13/02/2007	Quality review, legal issues contribution	P. Wilson
2	14/02/2007	Final review	Y. Legré
2.1	30/04/2007	Ethical issues contribution	P. Wilson
2.2	30/04/2007	Addition of references	V. Stroetmann
2.3	30/04/2007	Addition of legal annexes	I. Andoulsi
2.4	01/05/2007	Compilation and editing of all parts	C. Van Doosselaere
2.5	01/05/2007	Review	P. Wilson

3	02/05/2007	Editing	C. Van Doosselaere
3.1	03/05/2007	Comments by editorial team	N. Jacq
3.2	10/05/2007	Final editing	C. Van Doosselaere
3.3	25/05/2007	Editing and implementation of additional comments by N. Jacq	C. Van Doosselaere
3.4	05/06/07	Legal commenting	J. Herveg, I. Andoulsi
3.5	05/06/07	Editing and implementation of comments	C. Van Doosselaere
3.6	20/06/07	Final editing and release	C. Van Doosselaere
4.0	04/07/07	Final version	N. Jacq

Table of Contents

1. INTRODUCTION

1.1. PURPOSE

In D4.1 “Ethical, Legal, Socio-Economic Aspects of healthgrids: Baseline” [R1], we set out in some detail the existing EU level legal tools as well as economic principles that are important in understanding the potential bottlenecks for healthgrids in Europe.

We began to explore legal issues that might affect the uptake and deployment of healthgrids in the EU, in particular legislation on Data Protection, on Liability for Goods and on Services and Intellectual Property Rights.

Legal and regulatory issues are only one side of the non-technological challenges to implementing healthgrid based solutions in Europe. Planning effectively to get the most out of this technology requires a thorough understanding of the economic and social drivers that impact on the uptake of healthgrids. D4.1 thus also began to look at the factors that a thorough healthgrid roadmap should take into account if it is to be effective in supporting further development and ultimately uptake of grid-based computing in the health sector.

We came to certain broad conclusions in our first deliverable:

- EU-level legislation on **data protection** is adequate but not ideal for promoting healthgrids. When healthgrids are used for treating patients or planning care, the requirements of the legislation provide that, if the data are collected and processed by medical professionals, the balance of rights weighs in favour of data collection. That is, it is assumed that the patient’s general interest in obtaining treatment or advancing medical care outweighs his interests in privacy. The current legislation is not, however, adequate to support

most of the longer running research initiatives around which healthgrids are based.

- Our examination of the EU level legislation on **liability for goods and services** showed that the legislation is not at all adapted to the healthgrid domain. One of the reasons for this is, of course, that health services are organised at national or regional level and that the European Union has no legal competence to draw up legislation that states specifically how a health service should be organised.[1] However, the EU does have a range of legislation designed to protect citizens from harm resulting from goods offered on the market. Steps could be taken using guidelines, or even specific legislation, to address distributed computing services, such as healthgrids, which would seem at present to be only marginally covered by the existing rules. Accordingly it is important the existing European framework of general product safety is re examined to consider its applicability to distributed networks such as healthgrids.
  - There is a question as to whether EU legislation on **medical devices** applies to healthgrids. While it may be argued that a healthgrid could fall within the ambit of the current Medical Devices Directive in that it is a software tool that impacts on a medical act, the whole construction of the Directive is based upon physical goods (which might have a software component) placed on the market for purchase or lease. The Directive is therefore ill adapted to deal with the shared domain of grid-based services where software sold and owned by a wide range of participants in a grid initiative.
  - It would seem therefore that at present the only real way to have clarity over liability for the possible negative effects of healthgrids is through tightly constructed **contracts in private law**.
- However, to move healthgrids beyond the domain of university led and funded research tools we would need to address squarely the need to develop robust tools for sharing

[1] Treaty of the European Union Art. 152 provides that matters of health services organisation are subject to the rule of subsidiarity and limits the role of the EU to support and co-ordination.

of the **intellectual property** inherent in the design and population of a healthgrid application.

- In terms of **economic analyses**, we identified two main issues affecting eHealth investments in general: the benefits are often non-financial, which thwarts eHealth investments that should be made from an economical point of view; and many potential investors, in particular healthcare provider organisations, do not realise what the scope of the benefits to themselves might be.
- **Ethical considerations** run in the background of all of these issues: in the application of laws to healthcare systems, in the consideration of socio-economic issues, and in the organisational changes that might affect any relation with a patient.

Thus, in D4.1 we looked at the principles of healthgrids. The approach to D4.2 is at first a generic one, analysing these principles further and the SHARE vision, and exploring the ELSE issues that will need to be considered and 'dealt with' if they are not to become obstacles or roadblocks to the deployment and use of the technology.

This work includes a list of common challenges and bottlenecks from the baseline reports [R1 and R2], complemented by drawing up an initial view of the appropriate response from the research community (see also R3). Based on a storyline model approach, RTD activities to address these issues will be structured into a first version of the ethical, legal, social and economic components of the roadmap.

The purpose of D4.2 is thus to begin to map the ethical, legal and socio-economic issues onto the main technological milestones (i.e., computing grid, data grid, knowledge grid), in order to build towards a comprehensive roadmap for healthgrid development in Europe.

1.2. APPLICATION AREA

The document is intended for internal and external use. It will be also used as a dissemination tool for the SHARE project.

1.3. REFERENCES

[R1]	D4.1 A Legal, Regulatory and Economic Baseline for Developing a Roadmap for the Adoption of grid Technology in Healthcare http://eu-share.org/deliverables.html
[R2]	D3.2 Baseline on Technology and Security Aspects of healthgrids http://eu-share.org/deliverables.html
[R3]	D3.3 Bottlenecks & Challenges and RTD Responses for Technological and Security Aspects of Healthgrids Roadmap http://eu-share.org/deliverables.html

1.4. DOCUMENT EVOLUTION PROCEDURE

This document will be updated incrementally via WP4 activity as new information becomes available.

Any comments or feedback should be sent to the authors.

1.5. SOURCES

- BEAUCHAMP, T.L. & CHILDRESS, J.F. 2001. *Principles of Biomedical Ethics,* 5th edition. USA: Oxford University Press.
- Article 29 Working Group on Data Protection. 2007. *Working Document on the processing of personal data relating to health in electronic health records (EHR).*
- Treaty on European Union, Article 152. *Official Journal C 191*, 29 July 1992.
- "Scenarios4Health - Scenarios for ICT-Enabled New Models of Health Care" project (IST-150644-2006-F1SC-DE).

Available from World Wide Web <http://www.scenarios4health.eu/>

- ETTNER, S.L. & SCHOENBAUM, M. 2006. "The role of economic incentives in improving the quality of mental health care", in ed. JONES, A.M. *The Elgar Companion to Health Economics*. UK: Edward Elgar Publishing.
- Council Conclusions on "Common values and principles in European Union Health Systems". Document (2006/C 146/01), *Official Journal of the European Union* on 22 June 2006, pp. 1-5.
- STROETMANN, K.A. JONES, T. DOBREV, A. & STROETMANN, V.N. 2006. *eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites*. Luxembourg: Office for Official Publications of the European Communities. (ISBN 92-79-02762-X). Available from World Wide Web < www.ehealth-impact.org>
- MANNION, R. DAVIS, H.T.O. & M.N. MARSCHALL. 2005. *Cultures for Performance in Health Care*. UK: Open University Press.
- KNIGHT, W. "Wear your heart on the screen". *The Guardian*, Thursday April 27, 2006.
- KENNEDY, D.M. 2001. *A primer on open source licensing legal issues: copyright, copyleft and copyfuture*. 20 St. Louis U. Pub. L. Rev. **345**. Available from World Wide Web <http://www.denniskennedy.com/opensourcedmk.pdf>
- MCGOWAN, D. 2001. *Legal implications of open-source software*. U. Ill. L. Rev. **241**.
- Open Source Initiative. Available from World Wide Web <http://www.opensource.org>
- ANDERSON, G. F. et. al. 2006. Healthcare Spending and the use of Information Technology in OECD countries. *Health Affairs*. **25**(3)
- MENACHEMI, N. et. al., 2006. Hospital Information Technology and Positive Financial Performance: A different approach to ROI. *Journal of Healthcare Management*. **51(**1)

- JACOBS, R. SMITH, P.C. & STREET, A. 2006. *Measuring Efficiency in Health Care*. UK: Cambridge University Press.
- HERVEG, J. 2007. *La gestion des risques spécifiques aux traitements des données médicales en droit européen*. To be published.
- Council of Europe. Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted on 28 January 1981.
- Council of Europe. Recommendation R(97)18 of Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997.
- Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and free movement of such data. *OJ* L 281, *of 23 November 1995, 31-50.*
- Consortium of GEMSS project (IST-2001-37153). 2001. *GEMSS – grid-enabled Medical Simulation Services and European Law – Final Report on all the legal issues related to running GRID medical services*. Available from World Wide Web <http://www.ccrl-nece.de/gemss/Deliverables/D6.3b.pdf>
- HERVEG, J. 2006. "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in Healthgrid" in HERNANDEZ, V. et al. *Challenges and Opportunities of healthgrids, proceedings of Healthgrid 2006*. Amsterdam: IOS Press.
- Consortium of "Legally eHealth" study (European Commission Contract # 30-CE-0041734/00-55). 2006-2007. *Processing Medical Data: Data Protection, Confidentiality and Security*. To be published.
- Article 29 Working Group on Data Protection (a.k.a. "Working Party 16"). 1999. Recommendation 1/99 on Invisible and Automatic Processing of Personal data on the Internet

performed by Software and Hardware. Adopted on 23 February 1999.

- Council of Europe. Recommendation R(97)5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997.
- ACGT ("Advancing Clinico-Genomic Clinical Trials on Cancer") project (FP6-IST-026996). Available from World Wide Web <http://www.eu-acgt.org/>
- HERVEG, J. and POULLET, Y. 2007. *Which major legal concerns in future e-Health?* e-Health and Health Policies, Synergies for better health in a Europe of Regions, Plenary session: e-health and new social dilemmas. To be published.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *O.J. L 201*, of 31 July 2002, 37–47.
- Consortium of "Legally eHealth" study (European Commission Contract # 30-CE-0041734/00-55). 2006-2007. *Product Liability and Consumer Protection*. To be published.
- Directive 2001/83 of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use, *O.J. L311,* of 28 November 2001, 67-128.
- Council Directive 85/374 of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *O.J. L210,* of 7 August 1985, 29-33.
- Directive 1999/44 of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantee, *O.J. L171,* of 7 July 1999, 12-16.
- Directive 1997/7 on the protection of consumers in respect of distance contracts, *O.J. L144,* of 4 June 1997, 19-27.
- IAKOVIDIS, I. 2006. *eHealth & Patient safety, Myths, Visions and Realities*. Brussels: eHealth Congress, 19 October 2006.

- KOHN, L.T., CORRIGAN, J. & MOLLA, S.D., Editors; Committee on Quality of Health Care in America, Institute of Medicine. 2000. To Err is Human: Building a Safer Health System. Institute of Medicine
- STARFIELD, B. 2000 "Is US Health Really the Best in the World". *Journal of the American Medical Association*. **284**(4).
- BRETON, V., BLANQUER, I, HERNANDEZ, V., LEGRE, Y. and SOLOMIDES, T. 2006. "Proposing a roadmap for healthgrids", in HERNANDEZ, V. et al. *Challenges and Opportunities of healthgrids*. Amsterdam: IOS Press.
- Directive 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety. *O.J. L11*, of 15 January 2002, 4–17.
- Directive 2002/95 of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, *O.J.* L37*, of 13 February 2003, 19-23*.
- Council Directive 93/42 of 14 June 1993 concerning medical devices, *O.J. L169,* of 12 July 1993, 1-43.
- Meddev. 1994. *Guidelines relating to the application of Council Directive 90/385/EEC on active implantable medical devices and Council Directive 93/42/EEC on medical devices*. Available from World Wide Web <http://ec.europa.eu/enterprise/medical_devices/meddev/2_1-1__04-1994.pdf>. See also on World Wide Web <http://ec.europa.eu/enterprise/medical_devices/meddev/index.htm>
- Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J. L178,* of 17 July 2000, 1-16.
- Communication COM(2002)0667, final, from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of Regions. 2002. *eEurope 2002: Quality Criteria for Health related Websites*.
- Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-

consumer commercial practices in the internal market. *O.J. L149,* of 11 June 2005, 22-39.

- Directive 97/7 on the protection of consumers in respect of distance contracts, *O.J. L144,* of 4 June 1997, 19-27.
- SOLOMONIDES, T. 2006. *Structuring and supporting Healthgrids Activities and Research in Europe (SHARE): towards a European Healthgrid*. Amsterdam: e-Science 2006, 4-7 December 2006.
- VILCHES ARMESTO, L and LAURENT, P. 2006. "Intellectual property on medical data chimaeras and actuality". *Acts of the 16th World Congress on Medical Law*, Toulouse, 7-11 August 2006, p. 747-754.
- Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases. *OJ. L77,* of 27 March 1996, 20-28.
- Ray K. HARRIS, R.K. & STONE ROSENFIELD, S. 2005. "Copyright Protection for Genetic Databases". *45 Jurimetrics*.
- VANLANGENDONCK, P. "Le dossier médical électronique : problèmes de vie privée et de responsabilité". Available on World Wide Web <http://www.droit-technologie.org>
- Green Paper COM(95)382, final, from the European Commission. 1995. *Green Paper on copyright and related rights in the Information Society.*
- Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, O.J. L 122*, of 17 May 1991, 42–46.*
- Report COM(2000)199, final, from the Commission to the Council, the European Parliament and the Economic and Social Committee. 2000. *Report on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs*.
- Council Directive 93/98/EEC of 29 October 1993 on harmonising the term of protection of copyright and certain related rights, *O.J. L290*, of 24 November 1993, 9-13.
- European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of

copyright and related rights in the information society, O.J. L 167*, of 22 June 2001, 10-19.*

- World Intellectual Property Organisation. WIPO Copyright Treaty. Adopted in Geneva on 20 December 1996. Available from World Wide Web <http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html>
- World Intellectual Property Organisation. WIPO Performances and Phonograms Treaty. Adopted in Geneva on 20 December 1996. Available from World Wide Web <http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html>

2. EXECUTIVE SUMMARY

The objective of the SHARE project is to map key RTD (Research and Technology Development) actions that need to be taken at EU level to focus and advance healthgrid solutions meeting the needs of European and global medical and health-related research, health policy priorities, and of healthcare providers, thereby supporting the delivery of safe, high quality health and social care to European citizens, and also meeting foreseeable future challenges. In this way the study will prepare the ground for improved uptake of healthgrid technology.

Building directly on the ELSE (Ethical, Legal and Socio-Economic issues) Baseline Report [R1], this deliverable identifies the key challenges in the development of healthgrid solutions in Europe from the perspective of ethics, laws and regulations and socio-economic questions, including those that may be an impediment to the full exploitation of the technology. In this deliverable, the ethical, legal and socio-economic issues begin to be mapped onto the technology roadmap [R3], building towards a comprehensive roadmap in WP6.

While grid technologies are potentially of considerable added value for health research, the SHARE vision sees healthgrid applications of use to a wide community of varied stakeholders, including the (software) industry, insurances/payers, hospital management, (inter)national authorities, clinical professional organisations and the research community. In the long run, the list of stakeholders would extend to the patient, as healthgrids are deployed through various applications into medical practice. This deliverable, and the project in general, therefore seeks to go beyond ‘just’ the research community. Hypotheses of potential ELSE roadblocks on the way of healthgrid development will be exposed to be addressed in the WP5 application test cases, which will model the use of grid technology in two domains: epidemiology and innovative medicine.

In addition to potential obstacles and barriers, studies on efficiency and improvement of care chains are also described, as are economic and financial issues (benefit/cost considerations). The potential of healthgrid solutions needs to be understood by a wide user community if the technology is to be sought, applied, and developed in a sustainable manner. In other words, it is important to consider the 'pull' for the technology, and WP4 seeks to make the attractiveness of the technology understood by a wide user community – the language of this deliverable, as well as that of other WP4 deliverables, seeks to be as simple and non-technical as possible, even when delving into complex issues of law, ethics and economics.

The healthgrid roadmap will cover the domain of RTD and uptake of grid applications in healthcare comprehensively, including infrastructure, security, legal, financial, economic and other policy issues.

3. ETHICAL, LEGAL & SOCIO-ECONOMIC ROADMAP – A GENERIC APPROACH

The approach to the SHARE ethical, legal and socio-economic (ELSE) roadmap is illustrated in the Figure 1 below.

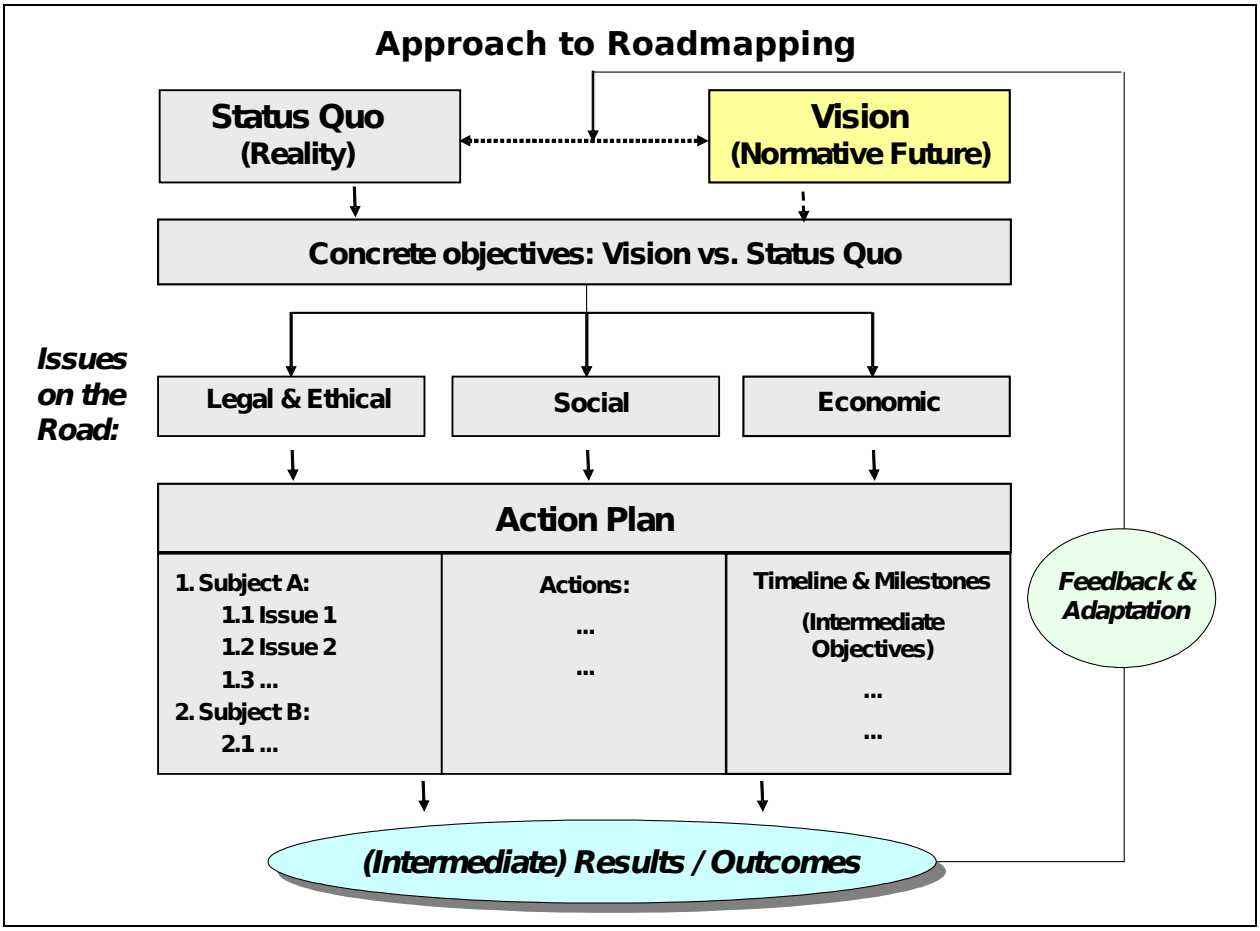

Figure 1 A Generic Approach to Roadmapping

This first ELSE roadmap aims to identify the relevant legal, ethical, social and economic issues as well as possible methodological approaches (and the stakeholders involved) that could be approached in the uptake of healthgrids vis-à-vis these issues. In this way, we begin to map the ELSE issues on the

technology milestones, identified as follows in the Technology Baseline [R3]:

- MD1 (Milestone Deployment 1), called *"Computing grid"*, corresponding to the successful permanent deployment of computing grid nodes inside European medical research centres;
- MD2, called *"Data grid"*, corresponding to the successful permanent deployment of data grid nodes inside European medical research centres;
- MD3, called *"Research K-grid"*, corresponding to the successful permanent deployment of knowledge grid nodes inside European medical research centres;
- MS1 (Milestone Standard 1), called *"grid DICOM"*, corresponding to the production of a standard for the exchange of medical images on the grid;
- MS2, called *"grid EHR"*, corresponding to the production of a standard for the *exchange of Electronic Healthcare Records* on the grid.

These milestones, as identified by the SHARE project team, correspond to important steps forward in grid services offered to the medical research community. Starting from services made available on the existing grid infrastructures, a persistent distributed environment for medical research has to be built. This environment will progressively be enriched with new functionalities as technology progresses.

It should be noted that these milestones reflect the current focus of the consortium team on grid infrastructure for medical research and not on healthcare practice. In the former case adoption of grids is less dependent on the evolution of EC legal regulations.

Based on these first milestones, an action plan on how to address these issues and the respective timeline to achieve the desired solutions can be developed. As reflected in the figure, the use of the roadmap will require that the intermediate

outcomes be analysed and the results fed back to adapting the objectives and actions correspondingly.

WP4 begins to address the use of healthgrids by a wider community, as reflected in part by the “healthgrid Story” (see Chapter 6). In the baseline report and in its first roadmap, ELSE issues begin to pose the questions that will require answers as healthgrid technology moves from an internal research core to more widespread applications.

The findings from our Baseline Report are reflected and further developed in this first Roadmap Report, supported by a “healthgrid Story”. This allows issues to be further analysed and first insights into required actions to be gained. In a next stage, this will be enhanced through an analysis of concrete successful projects, probably Mammogrid and WISDOM, and integration of parallel research and analysis within other SHARE Work Packages. In particular, this will be the Technology Roadmap and Use Case Reports on Epidemiology and Innovative Medicines.

This process is illustrated in the following Figure :

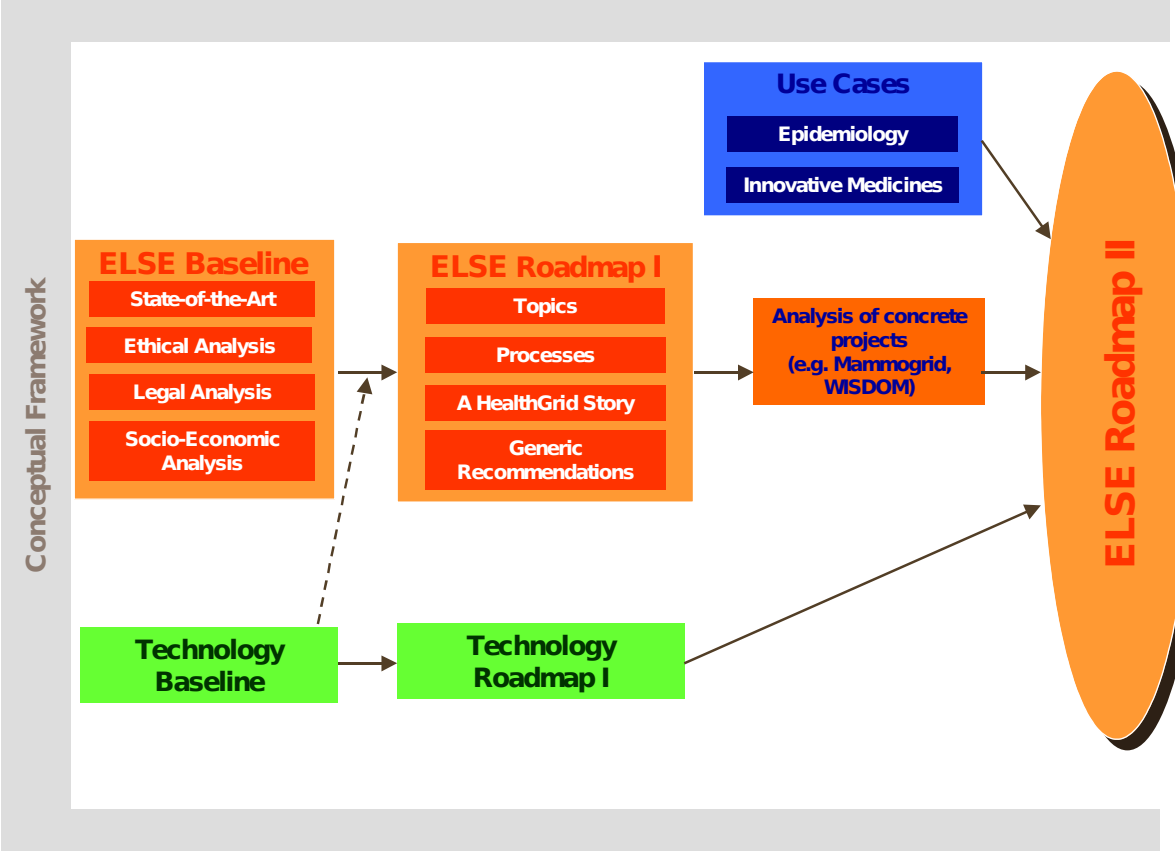

Figure 2 Developing the ELSE Roadmap – a Process View

To summarise, the following steps will be preformed to develop the basis for ELSE Roadmap I:

- Initial identification of subject topics, issues, processes
- Detailed discussion of relevant ELSE issues based on a "healthgrid Story"
- Generic recommendations.

In a next step, a further refinement of relevant issues will follow, combined with

- Analysis of concrete projects (e.g., Mammogrid, WISDOM)
- Identification of ELSE issues in the context of the two use cases – epidemiology and innovative medicines.

For instance, in the case of epidemiology (D5.1a) the following specific constraints have been identified:

- Legal regulations restrict the storage and use of personal electronic data.
- Obtaining patient consent for population-level information could be unmanageable and encryption techniques for large population data inefficient and even fragile. Anonymisation[2] and data dissociation appear to be a more realistic approach.

Other issues that must be resolved include:

- Traceability of accesses. Access to personal data must be traceable during the integration process and at least while the private information has not been removed. This is compulsory due to European and national regulations, which require identifying the potential leakages of privacy and the responsible persons.
- Management of patient consent. Requesting a patient's consent must clearly outline the usage of the medical data for epidemiological studies.
- Traceability of pseudo-anonymised data. It must be possible for the data subject or closely related persons to revoke permission of using the data in the future. It is therefore imperative to keep track of the modifications to the data.

Finally, the results of this process will be integrated in a final deliverable (D4.3) – ELSE Roadmap II – and built into SHARE's final deliverable, D6.2, the integrated roadmap.

[2] Currently, the law stipulates that **anonymisation** is the only way to ensure that data are totally detached from the identity of the patient. **Pseudo-anomynisation** does not entirely break the link between the information and the patient, in that it is always technologically possible to reverse the key used to pseudo-anonymise the data.

4. THE HEALTHGRID VISION AND THE SHARE PROJECT

The long term goal of healthgrids is to offer to healthcare professionals an environment created through the sharing of resources, in which heterogeneous and dispersed medical data, as well as applications, can be accessed by different users as a tailored information-providing system, depending on their authorisation, and without loss of information. Such an environment should thus enable primary data and resources to be accessed differently (and correctly) by different users, while further allowing for secondary use of the data and access to the resources to the research community involved in medical & life sciences.

The SHARE project aims to develop a European roadmap to enable the realisation of this vision, looking in particular at the technology developments required for the take-up of the technology. While the recent emergence of grid technology in the world has opened up new perspectives in interdisciplinary research and technology development at the crossroads of medical informatics, bioinformatics and system biology impacting healthcare, the potential for this technology is all the greater in the EU as Member States begin to face increased citizen mobility. There is thus an ever-increasing need for cross-border interoperability of data, cross-border infrastructures, optimal exploitation of resources (both technical and medical), and definition and implementation of standards in order to ensure an equitable distribution of health and social care, respecting the overarching values of universality, access to good quality care, equity and solidarity as well as the operating principles upon Member States' health and social systems are based (quality, safety, evidence-based care, ethics, patient involvement, redress, and privacy & confidentiality).

Grid technology responds to this need for pooled resources and sharing of geographically distributed data. However, as with any emerging technology, the use of grid also poses some

questions, especially when applied to such a sensitive field as that of medicine and health.

While the technical components of the SHARE project look at necessary technology developments necessary for the deployment of healthgrids, the ethical, legal and socio-economic components of the project examine the questions that the use of these technologies might imply. What provisions does EU-level law (with its application at national level) make for the processing of data, especially when it concerns such sensitive information as personal details and/or health-related data? From an ethics perspective, how do thousands of years of medical practice change (or not) in the age of eHealth? In the face of increasing pressures and expectations, how can health systems afford to invest in a new technology, with all the organisational changes that implies? Can they afford not to do so? And practically speaking, what will these technologies mean for the end users: the health and social care professionals, and the research community? How will they do their work differently and how will this difference make their work easier or better?

5. STATUS QUO

5.1. ISSUES IDENTIFIED IN BASELINE AND FRAMEWORK REPORTS

5.1.1.Introduction

In our ELSE Baseline Report we have explored the relevant EU level legislation that may be said to have some impact on the use of healthgrid technology in the European healthcare field through a series of questions and answers. We have set out a number of social and economic issues impacting on healthgrid uptake and have also provided an introduction to fundamental principles of biomedical ethics. These starting points are summarised below, before creating an initial catalogue of issues for further work.

5.1.2.Ethical issues in the use of healthgrids

In our Baseline Report, we introduced medical ethics, citing in particular Beauchamp and Childress' *Principles of Biomedical Ethics*[3] first published in 1979 and now in its fifth edition (2001). In this book the authors set our four principle of ethical behaviour in medicine and biomedical science:

- Autonomy
- Beneficence
- Non-Malfeasance
- Justice

In order to revisit these points we consider briefly the extent to which these core principle may pose questions for the healthcare practitioner wishing to use a healthgrid application.

5.1.2.1.Autonomy and healthgrids

Autonomy is intimately tied up with the legal duties of consent and confidentiality. Both however could prove difficult in the context of healthgrids.

[3] BEAUCHAMP, T. and CHILDRESS, J. *Principles of Biomedical Ethics*. Oxford University Press, USA; 5th edition (February 15, 2001)

The first question to ask therefore is whether the use of a healthgrid in the provision of care to a specific patient would require special consent. Looking at the example of the Oxbridge Cardiac Care grid (See Chapter 5), we can see that the doctor intends to submit the patient's data to a grid application in order to get assistance with the diagnosis. We will discuss later the need for consent to share the data in this way, but first must establish if the use of the grid application as such requires special ethical and legal consideration. Here the question is really one of the impacts the use of a grid-based tool has on the patient. Ethically we are looking at autonomy: is the patient's autonomy compromised by not fully understanding the technologies being used in providing care? Generally it is accepted that if a doctor uses state-of-the-art medical technology in the conventional way then a patient, in consenting to the care provided by that doctor, is consenting to the use of such technology. Thus, we do not expect a cardiologist to obtain special consent for using an electrocardiogram (ECG), nor a radiologist for using magnetic resonance imaging (MRI).

Two caveats should however be observed. If the technology could create harm to the patient, special consent should be obtained, since respecting autonomy means providing sufficient information so that the autonomy of the 'informationally' weaker party can be exercised. Thus, the risks of an epidural anaesthetic must be explained before the needle is inserted. The same argument exists if the risk is social rather than medical. Thus testing for a genetic condition that is not amenable to treatment requires prior consent since knowledge of possessing such a gene will be a burden to the patient and might also affect rights to social goods such as health insurance and mortgages.

For us then the question is if the use of a grid application *per se* falls into these special categories. We would propose two guidelines here:

1) If the use of a grid based tool is simply a way of getting a more complete diagnosis and moreover if it constitutes a reasonable use of medical expertise then no special consent would be ethically required;
2) If the use of the grid based tool could expose the patient to any risks such risks must be disclosed and special consent would be required.

We can see thus that the extent to which the grid poses a special ethical problem is not around consent to the use of the technology itself, but rather in consent to the sharing of medical information in the context of the duty of confidentiality.

The legal requirements of confidentiality have been extensively discussed in the Baseline on Ethical, Legal and Socio-Economic Issues [R1]. Here we look at the ethical aspects of that duty. If submitting a patient's information to a grid based application in any way might allow other people to identify the patient, his or her autonomy is compromised.

Thus in healthgrids, one of the key ethical issues will be in the possible compromise of the patient's autonomy that will arise from sharing his or her data with people who are yet to be identified. It is worth noting that it has been argued, notably by the European Article 29 Data Protection Working Party[4], that consent has only a very limited place as a justification of the sharing of health related data in the electronic age. The Member States' data protection commissioners note, with particular reference to the development of Electronic Health Records systems that seeking a patient's consent to the sharing of information is not easily justified when to do so would be asking the patient to opt for a lower quality of care. They argue therefore that robust system of security of information and

[4] Article 29 Working Group on Data Protection. Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131.

ethical practice should be adopted in which patients will be able to trust, notwithstanding that their information is shared, and providing for special opt-out possibilities when the nature of the information is especially sensitive.

In the development of healthgrids, we must therefore develop good ethical guidelines on how to share information, including the use of anonymisation and pseudonymisation wherever possible as well as general information campaigns which will make patients more aware of the way their information may be shared so that if they feel the need to do so they will know when and how to refuse to allow such sharing to take place.

5.1.2.2.Beneficence and Non-Malfeasance

As the Oxbridge Cardiac Care grid case explores, the importance of the application lies in supporting the healthcare professional's decision so that he or she may be better equipped to do good and avoid doing harm. As such, one could thus argue that a healthcare professional, in acting ethically, would indeed be obliged to use suitable grid applications if they were available. A healthcare professional refusing to use standard medical technology such as a sphygmomanometer or refusing to prescribe antibiotics would be considered in breach of his or her duty of beneficence, thus, as the sophistication of grid aided diagnosis develops we will one day arrive at a time when a healthcare practitioner not linked to the appropriate grid networks will be in breach of his or her duty.

However, until we have reached a time when grid applications are stable, well 'fed' with data and fully integrated into the evidence base of good clinical practice such arguments will not apply. At present, in the more experimental stages of the healthgrid it will be important to ensure that the use of the applications does no harm, but perhaps most importantly to ensure that the patient is aware of any possible medical and social risk (such as breach of confidentiality) so that the

applications can continue to develop without allegations of breach of ethical duties.

5.1.2.3.Justice

The ethical principle of justice concerned with the duty to achieve a fair distribution of resources as well as the need to develop an overall just medical system in which the greatest health of the greatest number is achieved is the principle of justice. It is in the respect for this principle that the greatest potential ethical benefit of healthgrids lies. The developments of applications such as Mammogrid have established that the sharing of a very large number of mammogram images across a wide network that allows radiologists to test suspect images against a known and tested database of cases significantly contributes to the early detection of breast cancer. The healthgrid in this case not only acts to the benefit of the known patient whose suspect image is submitted to the tool, but to the overall health of the population.

It can be seen therefore that healthgrids pose many challenges on an ethical level, as well as on a practical legal level. It is of great importance therefore that research roadmaps for healthgrids provide not only for scientific development but also for social science research, which will allow us to further explore the extent to which the use of healthgrids can empower healthcare professionals to meet their four cardinal ethical duties of respecting autonomy, doing good and contributing to the justice in healthcare.

5.1.3.Legal Issues in the use of healthgrids

As described in the ELSE baseline, legal issues include legislation concerning Data Protection, Liability for Goods and

Services and Intellectual Property Rights. The socio-economic treatment of the topic deals with the wider social values of health and health systems and the key actors with social and economic interests in such systems.

In this section we present a brief overview of the key legal issues as outlined in the baseline. A full discussion on all the relevant EU level legislation is found in the three annexes to this report.

Looking back at the discussion on Data Protection[5], we can see that in broad terms the current EU level legislation is adequate but not ideal for promoting healthgrids. When healthgrids are used for treating patients or planning care, the balance of rights weighs in favour of data collection - that is, it is assumed that the patient's general interest in obtaining treatment or advancing medical care outweighs his or her interests in privacy.

The current legislation is not, however, adequate to support most of the longer running research initiatives around which healthgrids are based. As the current EU level legislation stands, Member States can enact specific legislation covering specific tools such as healthgrids in order to exempt scientists and medical practitioners using healthgrids from some of the more onerous duties of the Directive.

No Member State has addressed legislation to this particular issue and so healthgrids are burdened with onerous data protection requirements which could deter scientists from using adopting healthgrid technology and using its enhanced computational and data acquisition power.

[5] For a detailed legal analysis of the data protection issues, please see Annex I to this document dedicated to Data Protection, Confidentiality and Security Issues.

EU level legislation on Liability for Goods and Services is not at all adapted to the healthgrid domain[6]. One of the reasons for this is, of course, that health services are organised at national or regional level and that the European Union has no legal competence to draw up legislation that states specifically how a health service should be organised[7].

However, the EU does have a range of legislation designed to protect citizens from harm resulting from goods offered on the market. Steps could be taken using guidelines, or even specific legislation, to address distributed computing services, such as healthgrids that would seem at present to be only marginally covered by the existing rules. Accordingly it is important that the existing European framework of general product safety be re-examined to consider its applicability to distributed networks such as healthgrids.

Furthermore the law on medical devices is very unclear with respect to healthgrids: while it may be argued that a healthgrid could fall within the ambit of the current Medical Devices Directive in that it is a software tool that impacts on a medical act, the whole construction of the Directive is based upon physical goods (which might have a software component) that are placed on the market for purchase or lease. The directive is thus ill adapted to deal with the shared domain of grid based services where software sold and owned by a wide range of participants in a grid initiative.

It would seem therefore that at present the only real way to have clarity over liability for the possible negative effects of healthgrids is through tightly constructed contracts in private

[6] For a detailed legal analysis of the liability issues, please see Annex II to this document dedicated to liability issues in the use of healthgrid technologies.

[7] Treaty of the European Union Art. 152 provides that matters of health services organisation are subject to the rule of subsidiarity and limits the role of the EU to supporting and co-ordinating the activities of the Member States.

law. If however the use of healthgrids across EU and international borders in shared public/private initiative is to become a reality then steps should be taken to develop guidelines and possibly legislation to harmonise the legal expectations of all actors in a healthgrid. As an interim step to EU legislation in this area it could be suggested that a suitable body, such as the High Level Group on Healthcare, be established.

However, to move healthgrids beyond the domain of university led and funded research tools we would need to address squarely the need to develop robust tools for sharing of the intellectual property inherent in the design and population of a healthgrid application.

As the law currently stands the rules of copyright are very protective and could constitute an impediment in the implementation of healthgrids because they treat computer software as a copyrightable literary work, the same as a play or a novel[8].

Currently, the owner of the copyrighted software running a healthgrid has the exclusive rights to reproduce his work, prepare derivative works, distribute copies to the public, perform the work publicly and display the work publicly. Under these circumstances any natural or legal person would have to pay to use computer programs while they constitute one of the most important compounds of healthgrids. Given that most grid applications will depend on shared access to multiple-copyrighted programmes it is unlikely that such a model of copyright is useful in protecting the entirety of a healthgrid application.

[8] For a detailed legal analysis of the intellectual property rights implied by the implementation of grids, please see Annex III to this document.

An open standards approach to software co-development could help the development and implementation of healthgrids. The open source licensing model actually uses copyright and contract principles to retain control of the work while enabling its use effectively for free and could thus encourage use and development.

5.1.4. Socio-economic issues in the use of healthgrids

Legal fine tuning, whether through standardised contracts, special data sharing agreements or open source software development models, will be of little use in driving forward the development and implementation of healthgrids if the social and economic setting does not provide incentives or if it presents other barriers to development or use. As these issues have not yet been examined in detail, it is necessary to analyse these aspects of healthgrid settings thoroughly in order to develop fully weighed up cost-benefit and cost-utility assessments of the use of healthgrids in healthcare delivery. In particular, the social and economic drivers and barriers (notably private incentives) must be examined and, where necessary, altered by different levels of policy intervention – from awareness raising to direct financial support for specified initiatives.

From a *socio-economic perspective*, it becomes obvious that the uptake of healthgrid systems and solutions will also heavily depend on the extent to which they can help address problems and challenges of health systems[9]. Such impact is presumed, yet there is little evidence of its scope. Detailed analysis of existing applications, as well as ex-ante assessments of the benefits from the future use of healthgrids will be essential for mobilising the required will and enthusiasm among research funding entities, political organisations and society at large. Potential benefits include timesavings, particularly important in cases of potential pandemics, and access to better quality clinical and research data, leading to improvements in the quality of clinical outcomes. The methodological framework

[9] A comprehensive treatment of the subject of health systems challenges in forthcoming in a report to the "Scenarios4Health - Scenarios for ICT-Enabled New Models of Health Care" project (IST- 150644-2006-F1SC-DE), http://www.scenarios4health.eu/

developed and described in the matrix above can frame the search for evidence on benefits of this kind.

The same framework can also be used as the basis for addressing another inhibitor to a widespread adoption of healthgrid solutions – lack of (knowledge about) private incentives. A business case for the routine use of grid technologies in the health sector is essential for moving from project-based, exemplary utilisation to a widespread uptake of healthgrid based solutions. As has been acknowledged by the literature[10], private incentives play an important role in healthcare, and will also play a major role in this business case.

5.1.5. Organisational, social and cultural issues in the use of healthgrids

Social issues around healthgrid uptake (as with all ICT based solutions) include impacts on citizens and patients, the micro level, and on society and health systems, the macro level. Both at the individual and the societal level, issues like universality of availability of full healthcare services to all citizens, equal access to healthcare, and equal high quality of services rendered are key issues[11]. Geographic factors relate mainly to equal access to quality care independent of location of living. ICT-based systems pose new problems like access to EHR by insurance companies or employers, and even police and prosecutors. Opinions and attitudes of patient and citizen associations and lobbying groups, often magnified by the media, can have strong impacts through public (policy) discussions of these topics on the implementation and diffusion of healthgrids.

The organisational level is always complex. Perspectives, confirmed by two most recent research studies[12], include:

[10] for example, see ETTNER, S.L.and M. Schoenbaum. "The role of economic incentives in improving the quality of mental health care", in ed. JONES, A.M. "The Elgar Companion to Health Economics", Edward Elgar Publishing, 2006

[11] "Council Conclusions on Common values and principles in European Union Health Systems", Document (2006/C 146/01), *Official Journal of the European Union* on 22 June 2006, pp. 1 - 5

[12] STROETMANN, K.A. JONES, T. DOBREV, A. and STROETMANN, V.N. "eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites", Office for Official Publications of the European Communities, Luxembourg, 2006 (56 pp. - ISBN 92-79-02762-X),

- Changing care pathways that need new information, skills, knowledge and process in healthcare providers
- Changing roles of healthcare professionals, teams and healthcare organisations
- Transfer of roles between healthcare professionals, teams and healthcare organisations
- Increased collaborative working and exchange of information between providers
- New relationships between citizens and healthcare professionals and organisations
- New strategic partnerships for third party payers and healthcare providers.

Again we have the situation that such issues will have an impact on whether and how healthgrid applications are taken up, and the potential implementation will often dramatically impact on organisational structures at the level of healthcare provider organisations, at the regional level on relationships and interactions among healthcare provider organisations (HPO), and also at the health system level (like globalisation of healthcare services). Looking at another dimension of organisational issues, work flow/process organisation will equally be impacted upon.

Finally, cultural issues are a key factor in health services[13], including the great diversity of attitudes, behaviour and knowledge exchange among professional and non-professional staff involved in healthcare, and the impact this has on the quality, efficiency and processes of services. Education and training, professional standards and bodies, rules and regulations, attitudes and behaviour all have an influence here.

available on www.ehealth-impact.org; "Scenarios4Health: Scenarios for ICT-Enabled New Models of Health Care", forthcoming on http://www.scenarios4health.eu/

[13] MANNION, R. DAVIS, H.T.O. and M.N. MARSCHALL "Cultures for Performance in Health Care", Open University Press, 2005

5.2. PRELIMINARY ISSUES CATALOGUE

This section summarises the most important domains of issues in each of the three principal dimensions of the roadmap: legal (and ethical), social and economic.

The legal and ethical issues include:

- Data Protection (legitimacy, multiple data controllers, medical and non-medical access, quality of data, security and confidentiality, data subject's rights, transfer of personal data outside of the European Union, etc.)
- Liability for Goods and Services (use of automated decision support in health service provision…)
- Intellectual Property Rights (healthgrid operating systems, applications and models, collections of medical data, etc.)

An initial list of economic issues is as follows:

- Cost-benefit and cost-utility analysis
- Benefits to patients, professionals, organisations and health systems
- Costs to patients, professionals, organisation and health systems

Finally, social issues include:

- Organisational inertia and change management
- Training, education and new skills requirements
- Collaborative working, new relationships and partnerships
- Cross-organisational resource deployment
- Process design and new care pathways
- Acceptance and culture of healthcare professionals
- Trust and confidence (automated decision support)
- Awareness and understanding
- Leadership and political support
- Policy development

6. A STORY MODEL APPROACH

In our Legal and Economic Framework Report we have set out, in some detail, all EU level legislation which may be said to have some impact on the use of healthgrid technology in the European healthcare field. To draw together the key issues highlighted and set out an inventory of potential bottlenecks we look at the issues once more in the context of a case vignette. The story outlined below[14] shows some of the potential uses of a healthgrid application in daily healthcare delivery and outlines the way in which the current European level legislation responds to the issues. The intention here is to go beyond the SHARE technology roadmap goal focusing on a grid environment predominantly for medical research, and to elaborate on potential impact not only for applying improved and new methods for diagnosis and treatment but also for routine trans-border, pan-European patient data exchange.

The story is presented twice below, once as a simple narrative, and once with key words highlighted and assessed for ethical, legal, social and economic issues.

Using the list of potential economic and legal bottlenecks highlighted by the story, and drawing also on more established applications such as WISDOM and Mammogrid, we present a roadmap of EU and national level actions necessary to support and accelerate the development and implementation of healthgrids in Europe.

6.1. A HEALTHGRID STORY OF TOMORROW

The following is a fictional episode from day-to-day medical practice showing a conventional response to a condition at the point of care:

> It's a busy morning surgery at a Madrid family practice when Dr. Maria Hernandez sees a pale

[14] Adapted from KNIGHT, W. "Wear your heart on the screen". *The Guardian*, Thursday April 27, 2006.

> clammy 50-something man, Mr. Sanchez, complaining of chest pain. An ambulance is called immediately. “I treat it as a heart attack until proven otherwise,” she says. “It’s protocol, and coronary heart disease (CHD) is the commonest cause of chest pain in middle-aged men. It’s also the commonest reason I call an emergency ambulance. It happens frequently.” In preparation for Sanchez’s arrival operating theatre staff are mobilised and the theatre reserved; the tests carried out in the ambulance and on admittance are not conclusive so that what follows is an expensive hospitalisation and with a high probability of risky medical intervention.

Here is an alternative story:

> It’s a busy morning surgery at a Madrid family practice when Dr. Maria Hernandez sees a pale clammy 50-something man, Mr. Sanchez, complaining of chest pain. She calls an ambulance. “I still have to treat it as a heart attack until proven otherwise,” she says. Dr. Hernandez explains to her patient that she would like to refer his case to her heart specialist colleagues in Oxbridge, UK. The Oxbridge group, in collaboration with institutions around the world, has already uncovered many secrets of this vital organ without opening up patients or running dangerous drug trials. They are creating a heart on a computer - a model - and subjecting it to all the stresses of modern life and watching how it responds, which is called the Oxbridge Cardiac Care grid (OXCCG). The model runs on healthgrid infrastructure.
>
> As she places the ECG leads on Mr. Sanchez, Dr. Hernandez points out how this model allows researchers to delve into the heart and witness events that are impossible to see without dangerous surgery. “You can see the outside of the heart, but ...

it's very difficult to get data from the inside," she says. She goes on to explain "the real beauty is that the complicated computing is hidden from the scientist. The researchers submit code though a portal interface. It puts all the data in the right place and pulls it back when you need to do things with it. The model of a patient's heart can be constructed very rapidly, making the day-to-day life of scientist a lot easier and providing an increasingly valuable service directly into clinical diagnostics. Scientists want to focus on the life science and clinicians need rapid results without having to think about how these big machines work."

The Oxbridge colleagues use the spare computing capacity of a large number of computers across Europe, including that of Dr. Hernandez, to conduct this scientific modelling. The results of this *in silico* modelling have recently become available for use directly in day-to-day clinical practice, and the harnessing of the enormous power of thousands of modern computers simultaneously allows a very rapid diagnostic response.

On the basis of the *in silico* modelling conducted by colleagues at Oxbridge Dr. Hernandez is able to diagnose that Mr. Sanchez in fact has a minor congenital abnormality and is not at risk of acute MI (myocardial infarction – "heart attack"). She cancels the emergency admittance and operating theatre preparations and informs and treats him instead for the mild chest infection that had caused the pain with which Mr. Sanchez originally presented. On the basis of data received from academic colleagues she is able also to inform Mr. Sanchez fully about the benign congenital heart defect.

Mr. Sanchez was so pleased that he managed to avoid a serious medical intervention on the basis of the advice his doctor got thanks to the healthgrid solution that he decided to write to the Minister of Health about the wonders of this new technology. He wrote, "It's not about arguing if there is a cost benefit that will pay off for the health of the nation. The question is simply one of making industry and government organisations aware of the possibilities. It's time we made all our doctors' and scientists' computers act as one giant computer, and put them to work for the patients. It doesn't even have to cost a fortune since they will just be sharing their collaborator's resources."

6.2. A HEALTHGRID STORY – ETHICAL, LEGAL, SOCIAL AND ECONOMIC ISSUES HIGHLIGHTED

6.2.1.Ethical and legal issues

6.2.1.1.Cross-Border Referral

Dr. Hernandez explains to her patient that she can ***refer his case to her colleagues in Oxford, UK*** *who, in collaboration with institutions around the world, is slowly uncovering the secrets of this vital organ without opening up patients or running dangerous drug trials. They are creating a heart on a computer - a model - and subjecting it to all the stresses of modern life and watching how it responds, which is called the Oxbridge Cardiac Care grid (OXCCG)*

In the story we see that Dr. Hernandez refers Mr. Sanchez' case to colleagues in Oxbridge running the Oxbridge Cardiac Care grid This means she is seeking advice on a Spanish patient from someone in another European Union country, is this legal and ethical?

Before even thinking about whether Dr. Hernandez can legally send Mr. Sanchez data to Oxford to obtain a second medical opinion, we should establish that Dr. Hernandez is processing his data legally. If this processing forms part of a filing system or is intended to form part of a filling system it will be covered by the Spanish Data Protection Legislation enacted in pursuance of the European Data Protection Act. Given that the medical records must be filed in some way, this would seem to be very likely, furthermore, If any automatic processing is used, such as and Electronic Health Record, then the rules of data protection will apply regardless of the nature of the processing.

We can assume that the processing of personal data is carried out by Dr. Hernandez is for the medical care and diagnosis of her registered patients. Accordingly such processing is covered by the rules concerning medical data and does not need the explicit consent of the patients if the processing is made by a health care professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (ex. secretary or assistant). Thus, although it is ethically correct that she has explained to Mr. Sanchez that she intends to send his data to Oxford she is not legally required to do so if she can ensure that the person to who the data will be sent is subject to a legal duty of secrecy.

However, Dr. Hernandez, acts as data controller, has a duty to inform her patients generally about the data processing she performs or others perform for her and to notify that data processing to the relevant national supervisory authority. Dr. Hernandez must therefore ensure that the data held are adequate (accurate) and that they are held securely and that confidentiality is respected.

As medical data have to be processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy any processing of data is conducted by staff other than health care

professionals, such as administrative staff, would have to be under a contractual or a legal duty of confidentiality which could result in termination of employment if confidentiality were broken. A policy access to the medical files should be created.

Thus we see that Dr. Hernandez has a legal right to collect and process the medical data of her patients in order to provide them with medical care.

Now, however, she wishes to communicate her patients' medical files to a third party, the Oxford University Cardiac Care grid (OXCCG) in order to provide her with decision support in order to better treat Mr. Sanchez.

Here we come to several legal and ethical questions. From a data protection perspective the first question to ask is whether such an operation on the patients' medical data is compatible and necessary with the initial purpose of the data processing by Dr. Hernandez to provide the patients' with medical care. Here Dr. Hernandez would need to show that the OXCCG allows her to give better care to her patients and therefore may be considered as necessary for the purposes of medical diagnosis and the provision of care or treatment.

The next question to address is how the sharing of Mr. Sanchez medical data with OXCCG should occur. Here it will be a question of how the OXCCG works. If the services of OXCCG could be provided on the basis of Mr. Sanchez' anonymised data then Dr. Hernandez should perform the necessary anonymisation and send only the anonymised data. It is unlikely however that this will be the way in which OXCCG works, because it is intended to provide Dr. Hernandez with patient-specific advice. Although on a technical level it is possible to render such data anonymous, it is very difficult to satisfy the legal rules for such anonymity, indeed some national Data Protection authorities do not accept the concept of medical data anonymisation at all.

Accordingly Dr. Hernandez will have to ensure that OXCCG process and store all identifiable data according to the law, that such data are processed only by people with a legal obligation of secrecy and that data are not held for longer than necessary. Dr. Hernandez would be well advised to have a legal contract between herself and OXCCG setting out these requirements. Dr. Hernandez should use the standard contractual clauses as provided by the Data Protection Directive to ensure an adequate level of protection.

If the OXCCG runs a portal accessible by registered practitioners any one of whom could see Mr. Sanchez record, it would be advisable to have the express written consent of the patient who confirms having been thoroughly informed about OXCCG processing and the access regime.

It can be seen therefore that from a Data Protection perspective the submission of a named patient's data to a healthgrid could be legally and ethically justified. It is established that so long as the data collected and processed by medical professionals, in a way necessary for the purpose of providing healthcare to that same patient, the balance of rights weighs in favour of data collection - that is, it is assumed that the patient's general interest in obtaining treatment or advancing medical care outweighs his interests in privacy.

However, many newly developed healthgrid applications currently running are not designed primarily to be used in care delivery to an individual patient but for different, longer term purposes – that is research, preventative medicine or healthcare planning. In addition, these applications are usually not controlled by medical professionals but by research

scientists. Furthermore, for the purposes of research, a great deal of data is stored per patient including an extensive medical history. This makes it a practical impossibility to render the data set anonymous. Where this is the case, Member States have the possibility to enact specific legislation covering specific tools such as healthgrids in order to exempt the scientist using running healthgrids from some of the more onerous duties of the Data Protection Directive.

Member States could, for example adopt specific legislation to encourage the linking of diagnosis-specific databases across a region or state in order to support research into a given disease. However, to date, no Member State has specifically addressed legislation to this particular issue. In this legal environment, healthgrids drawing the data and data processing power of many hospitals together are burdened with heavy data protection requirements which could deter scientists from adopting healthgrid technology and using its enhanced computational and data acquisition power.

Perhaps more significantly little attention has been paid to the specific needs of data sharing for healthgrids across European borders and outside the Union. If healthgrids are really to grow to their full potential and deliver their promise adjustments must be made to national and supranational legislations to re-assure would-be healthgrid users that it is legal to share health related data using grid technology. This in turn implies the development and adoption of robust guidelines developed specifically for the healthgrid context and that address the balancing of interests between an individual's privacy and medical advancement.

6.2.1.2.Reliance on an automated system – liability

She goes on to explain "the real beauty is that the complicated computing is hidden from the scientist. ***The researchers submit code though a portal interface. It puts all the data in the right place and pulls it back when you need to do things with it****. It's making the day-to-day life of the scientist a*

lot easier. Scientists want to focus on the life science without having to think about how these big machines work."

Dr. Hernandez explains the potential benefit of the OXCCG, saying that researchers submit code to a portal which pulls the right data together at a time she needs in order to help her make a diagnosis. We have already looked at the data protection issues here and have argued that special contracts will need to be put in place to ensure that the possessing of medical data by a third party is legal.

Dr. Hernandez's explanation suggests however that the next level of interaction she has with the OXCCG is based on automated data retrieval and aggregation. She is, in effect, making a medical diagnosis on the basis of a machine decision.

Legally this poses only small problems as long as no misdiagnoses are made. However, at a European level there is currently no legal guideline on how the liability should be shared – accordingly this is currently all subject to carefully drafted contracts which pre-define liability for possible mistakes. It may be argued therefore that the European Union should adopted either secondary legislation such as a Directive or at least common contractual guidelines for clarifying the cross border implication for shared care.

6.2.1.3.Cross-border and cross-institutional Licensing, IPR sharing

It's time we made all our doctors' and scientists' computers act as ***one giant computer,*** *and put them to work for the patients*.

This sentence that Mr. Sanchez writes to his Minister of Health describes a situation that might sound ideal, but legally it would in fact be rather difficult to set up.

If it appears that legally the rights of the patient and the copy-right the scientist will acquire on the database he created can coexist,[15] in practice a conflict may occur, especially between patients' rights and the personal data protection regime on one hand and the *sui generis* rights protecting a database on the other hand.

It may be argued that the patient's rights to the protection of their sensitive data are superior to the copyright of the scientists, which would have a direct impact on the exercise of authors' exclusive rights. In law the scientists, here legally the authors, could not prohibit to the patient the access to and the use of a copy of his medical record, since this is a right accorded the patient through Data Protection law. Thus, the authors (here the copyright owners) could not exercise their exclusive rights alone. Consequently the authors could not protect their

[15] To this extend see Recital 41 of the Directive 95/46/EC which states that *"(..) this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software"*. On the other hand, Recital 48 of the Directive 96/9/CE states that *" (...) the provisions of this Directive are without prejudice to data protection legislation"*. These texts show well that the European legislator had and still has some fears that one right might encroach on the other or that one of them might prevent the exercise of the other. It could be argued that, had the coexistence between both rights been easily made in practice, this cross-referencing in the text of the directives would not have been made.

interests in the databases and thus could not protect their work in the development of healthgrids.

On the other hand, there is a contradiction between the intellectual property rights and the needs of the grid technology, which would require that the access to databases and to programs of computer is free of rights.

The challenge for EU and/or national legislators is therefore the find a way of balancing the two competing sets of rights - for if they do not a full exploitation of grid technology in healthcare could be slowed down for long time.

As such, it might be desirable for the Commission to develop guidelines to the use of open licensing and open standards, which could address the tension between the intellectual property rights of developers and the needs of the grid technology. Such an open standards software approach could then be a solution to help the development and implementation of healthgrids. In the United States, the open source model (being a more open system than open standards) currently uses copyright and contract principles to retain control of the work and could thus encourage use without dedicating the work to the public domain.[16] Such a model could be adopted and developed into appropriate legal tools at the European level.

[16] See KENNEDY, D.M. "A primer on open source licensing legal issues: copyright, copyleft and copyfuture, *20 ST. LOUIS U. PUB. L. REV.,* 2001, 345, p. 359-360; MCGOWAN, D. "Legal implications of open-source software", *U. ILL .L. REV.,* 2001, 241, p.242-243. More generally see Open Source Initiative, at http://www.opensource.org.

6.2.2.Socio-economic aspects

6.2.2.1.Cost-Benefit Analyses

Mr. Sanchez was so pleased that he managed to avoid a serious medical intervention on the basis of the advice his doctor got from her colleagues that he decided to write to the Minister of Health about the wonders of this new technology. He wrote "It's not about arguing if there is ***a cost benefit that will pay off for the health of the nation****.*

Mr. Sanchez's statement relates to a crucial issue regarding the economic rationale for investing in deployment of Healthgrids – the distinction between private and social benefits.

In a market setting it is usually the main beneficiary of a service who pays, and investments are only made if adequate returns accrue to the party making the investment[17]. In healthcare, flows of benefits may diverge from flows of costs. "Private" benefits to investors may not provide sufficient incentive to invest in healthgrid, even though benefits to society may constitute a very substantial return.

From the perspective of Mr. Sanchez, the cost benefit argument is indeed obvious and does not require lengthy discussions – he has benefited greatly from the use of healthgrid at no extra cost. Of course, this is not the same for all stakeholders involved. The costs and benefits for Dr. Hernandez, and in particular the difference between them, are less clear. She can

[17] See ANDERSON, G. F. et. al., "Healthcare Spending and the use of Information Technology in OECD countries" in *Health Affairs*, Volume 25, Number 3, May/June 2006

only access the results from the healthgrid research at some cost, be it direct payment, giving access to her computing capacity, time for implementing the service into her work process, or a combination of these. Benefits may range from personal satisfaction to financial benefits. The people running the OXCCG face a completely different challenge – the investment in OXCCG build up and maintenance is their main cost. Their benefits from using the results as physicians, the same way as Dr. Hernandez, are unlikely to cover the investment costs.

This illustrates the complexity of the cost benefit argument when looked upon from the perspective of different stakeholders. When we turn to the so-called social benefits, i.e. benefits to society, the relevant items to consider will change again. The position of a policy maker, whether on Member State or EU level, should be that of a "social planner". So from their perspective, it is important to know whether healthgrids "will pay off for the health of the nation".

Different business organisation models for healthgrid services are possible and an important step towards deployment is choosing one in which private cost benefit ratios do not prove prohibitive to services worthwhile from the point of view of society.

Part of the relevant analysis should be concerned with the distinction between financial and economic costs and benefits. Recent research[18] shows that benefits from eHealth are often not cash. This makes achieving sustainability of investments even more difficult. Private investments decisions are made on the basis of the expected rate of financial return. This is not always guaranteed, especially when the benefits are quality of care or cost avoidance for extra health services. Voices for combining different analytical methods in support of decision

[18] STROETMANN, K.A. JONES, T. DOBREV, A. and STROETMANN, V.N. "eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites", Office for Official Publications of the European Communities, Luxembourg, 2006 (56 pp. - ISBN 92-79-02762-X), available on www.ehealth-impact.org

making, especially in areas where societal interest is considerable like the healthgrid area, are becoming louder[19].

6.2.2.2.Policy Development

The question is simply one of ***making industry and government organisations aware of the possibilities****.*

Making someone aware of a possibility is nowadays not sufficient, yet it is a good start. Indeed, industry and government organisations should be made aware of the potential that healthgrid has. The next step will be to convince decision makers that it is worthwhile to invest (not only financial resources, also time, effort, influence, etc.) in realising this potential. One argument can be build around the challenge to provide the best possible health service to as many people as possible, given the budget constraints. As the EU Council of Ministers agrees, "a primary ethical challenge is to balance the needs of individual patients with the financial resources available to treat the whole population"[20].

healthgrids are one of the options to address this challenge. It has to be compared to alternative options, so that an optimal choice of tools for addressing the challenge is made. Such an analysis must be one of the actions on the roadmap towards healthgrid deployment. Once the role of healthgrids is established, policy makers have to intervene, in that they change private incentives for uptake of the grid technology and services in health provision where necessary.

[19] MENACHEMI, N. et. al., "Hospital Information Technology and Positive Financial Performance: A different approach to ROI", Journal of Healthcare Management, 51:1, January/February 2006

[20] "Council Conclusions on Common values and principles in European Union Health Systems", Document (2006/C 146/01), *Official Journal of the European Union* on 22 June 2006, pp. 1 - 5

6.2.2.3.Cross-Border and Cross-Institutional Resource Allocation and Sharing, IPR and Patenting

It doesn't even have to cost a fortune *since they will just be sharing their collaborator's resources.*"

If data transfer is covered by existing purposes (flat rate internet access) and access to the service is exchanged for access to computer power (no payment for computer) then there is no expenditure incurred for use of the grid. This is consistent with results from the eHealth IMPACT study, which show that technical costs are often a relatively small part of a successful eHealth investment. What are often neglected are the change management and other organisational costs, which can constitute between 30% and 50% of the total investment cost[21]. If healthgrids are to be deployed successfully on a large scale, the organisational component, including changes in research, clinical, and working practices should receive a lot of attention.

It doesn't even have to cost a fortune since they will just be ***sharing their collaborator's resources****.*"

Assuming that the cost allocation issue is solved, for example in the way suggested above, there is still the question of sharing the outcomes. This is particularly relevant to the research applications, in the illustrative story this is the research conducted by the OXCCG. The Intellectual Property Rights and the patenting processes have to be solved on a legal basis. However, the behavioural aspect is no less important. The balance between competition and collaboration is difficult to

[21] Results from "eHealth IMPACT – Study on the economic impact of eHealth", Reports available on www.ehealth-impact.org

get right. On the one hand, the healthgrid philosophy is based on collaboration and positive results are only possible following that approach. On the other hand, the collaborating organisations are often in competition. For example, hospitals compete for patients paying higher rates, status, and recognition. Thus, a hospital may be reluctant to provide its facilities if they are likely to lead to success of its direct competitor in the same town.

This is not an unsolvable issue, yet it can prove a narrow bottleneck if not addressed in due time.

6.2.2.4.Reliance on an Automated System – Acceptance and Trust Technology and New Working Practices

"The real beauty is that the complicated ***computing is hidden from the scientist. The researchers submit code though a portal interface. It puts all the data in the right place and pulls it back when you need to do things with it.*** *It's making the day-to-day life of the scientist a lot easier. Scientists want to focus on the life science without having to think about how these big machines work.*"

In an ideal world, in which everything works the way it is intended to, this vision of the separation of roles is indeed appealing. In the real world, however, the statement of Dr. Hernandez opens the discussion on two critical features of using healthgrid services as described in the story. The first of them is confidence and trust in a highly complex technology solution. The second is the need for changes in the working practices of health professionals and researchers.

Submitting a set of data into the systems and receiving a result within a few seconds is a substantial improvement to a scenario

in which manual processing of the data takes days or weeks. The implicit assumption is that the result is of the desired quality in both cases. Even if technically this is the case, the challenge is to convince the users. Indeed, health professionals and scientists are usually not particularly interested in the technical details of computing. This also leads to an understandable sceptical attitude towards such technology. When the manual process is carried out by the scientist, he or she is confident in the results because of the understanding of how these have been derived. Lack of knowledge about the computing processes in a grid may thus lead to lack of confidence and trust in the derived results. This is in particular the case when grid processing is used for the purposes of acute healthcare treatment, where wrong analysis can lead to serious harm. Lack of confidence is likely to lead to reluctance by professionals to take up healthgrid services.

This reluctance may be further reinforced by the fact that uptake of such services requires, if it is to deliver the expected benefits, changes in clinical and working practices. For instance, Dr. Hernandez has to consult the OXCCG first, instead of reaching to the phone for an emergency ambulance. She must also be able to make her enquiry to the OXCCG quickly, as well as interpret the results in real time. Otherwise, the delay may be lethal for her patient in case he really is suffering a stroke. This issue has already proven critical in implementing various eHealth solutions[22]. Appropriate change management, leadership, and training have to be provided in order to avoid resistance to change to become an inhibitor to the deployment of healthgrids.

A further, related aspect is the perspective the third party payer, usually some form of health insurance organisation. The required new working practices are unlikely to fit the reimbursement schemes designed for the old ones. For

[22] see STROETMANN, K.A. JONES, T. DOBREV, A. and STROETMANN, V.N. “eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites”, Office for Official Publications of the European Communities, Luxembourg, 2006 (56 pp. - ISBN 92-79-02762-X), available on www.ehealth-impact.org

example, if Dr. Hernandez is paid according to set clinical pathways, she will be able to get her efforts reimbursed in case she makes a quick examination of Mr. Sanchez and calls the ambulance. In case she uses the OXCCG service, she will only be able to invoice the insurance company for the quick examination at the start, and then for further treatment after the diagnosis. She will have to cover the cost of making the diagnosis with support from OXCCG herself. Indeed, the marginal cost of making an enquiry to OXCCG, i.e. the cost of one extra enquiry once the system is in place, is nearly zero. The real cost, including a share of the associated development and maintenance costs of OXCCG, the training required to use the system efficiently, etc, is higher and someone has to bear it. Thus, if third party payers do not accept that changes in working practices associated with the uptake of healthgrids require changes in reimbursement schemes, such changes will be very difficult to achieve.

6.2.2.5.Decision-Making based on a healthgrid Processes

The results of this in silico modelling can be used directly in day-to-day clinical practice. On the basis of the results she receives from her colleagues at Oxford, Dr. Hernandez is able to diagnose *that Mr. Sanchez in fact has a minor congenital abnormality and is not at risk of MI. She informs him and treats him instead for the mild chest infection that had caused the pain with which Mr. Sanchez originally presented. On the basis of data received from academic colleagues she is able also to inform Mr. Sanchez fully about the benign congenital heart defect.*

Using healthgrid to receive instantly results that enable faster accurate decision-making is a desirable goal. Making the correct diagnosis in real time instead of treating according to a different, assumed diagnosis is certainly an improvement in the

quality of healthcare[23]. In addition, as in the case of Mr. Sanchez, it can lead to considerable cost savings.

The issue of relying on technology for decision-making in the health sector is not restricted to, yet highly relevant for healthgrids. At the heart of the problem lies the question of accountability. When everything is the way it is expected to be, the merits of the above scenario cannot be reasonably questioned. The difficulty arises when things go wrong. Who is accountable for a wrong diagnosis? Is it the doctor, who has trusted technology more that she should have? Or is the doctor blame free, as long as she has followed the correct procedures? This problem should be addressed from a society point of view and regulated from a legal perspective. Otherwise, the created uncertainly will lead to strong resistance on behalf of those who are to use healthgrid services.

[23] see for example, JACOBS, R. SMITH, P.C. and A. STREET, "Measuring Efficiency in Health Care", Cambridge University Press, 2006

7. CONCLUSIONS

The discussion above highlighted the important ethical, legal and socio-economic issues that have to be addressed on the way towards deployment of healthgrids. The analysis is preliminary, based on an invented, illustrative story and will be further developed on the basis detailed analyses of two running healthgrid solutions. Nevertheless, there are already certain recommendations that can be made. These can be seen as specific activities that will become part of the comprehensive roadmap for addressing legal, ethical, social, and economic aspects of deploying healthgrids across the European Union.

Broadly, these recommendations can be summarised as follows:

In terms of legal and ethical issues:

- A careful analysis of the full impact of data protection legislation on the potential for healthgrid development within the context of an ethical respect for privacy is needed;
- A stepwise approach to developing the liability framework distributing legal responsibility appropriately across the healthgrid users while providing legal certainty for all stakeholders, including patients, is required; and
- The balance between control over intellectual property rights and the protection of investments and the interest of a widespread and un-predefined community in interacting in the use of grid applications needs to be reconsidered.

Economic aspects of the use of grids in the health sector, as for any investment in the healthcare sector, will need to be rigorously explored to build a convincing case:

- An analysis of the extent of desirability of healthgrids is needed: what are alternative options for achieving the set goals?
- Also needed is an analysis of stakeholder perspectives and incentives, especially as regards financial implications of healthgrid uptake.
- It is likely that interventions aimed at adjusting private incentives will be necessary.
- Similarly, an adjustment of reimbursement schemes will likely need to follow to allow for sustainable uptake of new services that change clinical and working practices.

Finally, in order for the uptake and deployment of healthgrids to make a significant impact on the delivery of health services, social and behavioural issues must be addressed:

- Support and control the level of accurateness of results from using healthgrid processing;
- Ensure user confidence, based in particular on the above;

- Facilitate change by supporting training and further education related to using healthgrids; and
- Facilitate change in working practices by minimising uncertainty and reducing risk for users.

8. ANNEX I: DATA PROTECTION, CONFIDENTIALITY AND SECURITY ISSUES

Implementing a healthgrid generally implies the processing of a patient's personal health data.

In Europe, such data are protected at EU level by different legal sources and at national level by diverse national legislations. But although personal data are the object of numerous European legislations, the problem of the protection of these personal data (medical or not), still raises several questions that would be of importance in the implementation of healthgrids on the territory of the European Union, such as data processing, access rights for data subjects, free flows of personal data within the Member States of the European Union or data protection national legislations harmonization (see below Part I "Processing of Medical Data").

It is also true that as the confidentiality and the protection of patients' health personal data are governed by diverse

European rules, as well as by the requirements of ePrivacy legislation regarding communications infrastructure, in practice, the confidentiality requirements make healthgrids systems security critical (see below Part II "Network Compliance with Confidentiality and Security Requirements").

It is not so much the patient's health data processing that is aimed here, but the question of the healthgrid in itself. Indeed, when a telematic network is set up, it already presents, among other risks, risks for the patient's rights and the liberties. These particular risks are very often spent under silence or simply ignored[24].

8.1. PART I: PROCESSING OF MEDICAL DATA

The key principles relevant to the processing of personal data were first established by the Council of Europe[25], and further developed in Directive 95/46/CE of the European Union[26].

The latter is the major source of legislation[27], even if some Recommendations made by the Council of Europe are of importance for the healthcare sector and for the use of grid technology in that sector, since they are focusing on the field of medical data and scientific research[28].

The purpose of the Directive is to allow the free flow of personal data between the Member States of the European Union, in

[24] On this question and on the definition of particular risks see HERVEG, J., "La gestion des risques spécifiques aux traitements des données médicales en droit européen", to be published.

[25] Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1981; Recommendation No. R (97) 18 of Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997.

[26] Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and free movement of such data, *OJ L 281*, of 23 November 1995, 31-50.

[27] This is the reason why this text is analysed in particular. Further details of other documents governing medical data processing will be available in relation with the analysis of case scenarios.

[28] For an overview of all texts governing data processing, see Annex IV to document D4.2. See also *GEMSS – Grid-enabled Medical Simulation Services and European Law – Final Report on all the legal issues related to running GRID medical services,* 1-117.

order to facilitate the establishment and the functioning of the internal market.

The second objective of the Directive is to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of their personal data.

The protection granted by the Directive does, however, go further than the protection of the natural person's intimacy, i.e. generally speaking, the protection of each natural person's private life. It applies more particularly to any sensitive data relating to natural persons such as data concerning health, including mental health.

As stated by senior researcher Jean Herveg at the healthgrid Conference 2006, in Valencia, *"to be effective and coherent* (the Directive had) *to be built on the analysis of the risks capable to affect the fundamental rights and freedoms of the data subject.* (Indeed) *it is only possible to determine the conditions under which personal data can be processed in full respect of the fundamental rights and freedoms of data subjects when these risks are identified"* [29].

Prior to introducing the relevant provisions of the Directive that will impact the implementation of the grid technology for the

[29] HERVEG, J., "The Ban on Processing Medical Data in European Law: Consent and Alternative Solutions to Legitimate Processing of Medical Data in Healthgrid", in *Challenges and Opportunities of healthgrids, proceedings of Healthgrid 2006,* HERNANDEZ, V. and others, Amsterdam, IOS Press, 108.

biomedical sciences and in the healthcare sector (Part I C), we will begin by defining some key concepts (Part I A) useful in the application of data protection principles, outlining the scope of the Directive and presenting its principles relevant for medical data processing (Part I B).

The analysis will then come back on the specific cases of the transfer of personal data between the Member States of the European Union (Part I D) and of the transfer of such data to third countries located outside the European Union (Part I E).

Finally, some specific rules applicable to the processing of medical and genetic data not contained in the European Directive will briefly be presented (Part I F).

8.1.1.Part I: A: Key Concepts[30]

8.1.1.1.Personal data

According to Article 2(a) of the Directive, the term 'personal data' relates to *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".*

According to this definition, personal data might concern any information regarding data subjects such as their names, their

[30] For an overview of all the key concepts of the Directive, see the text of the Directive itself, art. 2; See also VEREECKEN, I. and HERVEG, J. *Legally e-Health: Processing Medical Data: Data Protection, Confidentiality and Security,* to be published.

e-mail addresses, their opinions, a sound or an image related to them, or their personal circumstances, whether these relate to their private, professional or public life.

Moreover, to be considered as personal data, data must relate to natural persons. Data strictly relating to companies, public bodies or other legal entities are not personal data. However, in some EU Member States like Austria, Luxembourg and Italy, data relating to companies are protected as personal data.

It is also important to underline that personal data might concern persons who are alive, but also dead persons at the time of the processing. However, in some of the Member States as in Ireland, in Sweden or in the United Kingdom, personal data only concern living persons.

Finally to be considered as personal data, data must allow direct or indirect identification of the data subject.

Data allowing *direct identification* of the data subject are data that can be easily related to a data subject and reveal his identity. This is the case with data such as names, addresses, dates of birth or even genetic data. These data when combined allow the identification of a data subject with a small margin of doubt.

Indirect identification requires further steps to make a link between a specific person and the data being processed.

Therefore, the fact that data cannot permit to establish a direct link with a particular data subject does not necessarily imply that they do not constitute personal data.

The possibility to identify a data subject through his data is assessed *in abstracto*[31]. In other words, the mere existence of a possibility to establish a link between the data and a particular person is being sufficient to determine that personal data are involved. Therefore, coded, anonymous or pseudonymous data are to be considered as personal data even if the data controller[32] does not have the code key to access the original data.

However, in some Member States, such as the United Kingdom, Ireland, Austria or the Netherlands, the possibility to identify a data subject through his data is assessed *in concreto*, which means that one should make his assessment taking into account the sole information which is or which is likely to be in the possession of the controller and could help him to identify the data subject.

[31] Indeed, Recital 26 of the Directive states *" […] to determine whether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person; […]".*

[32] See point 4 infra.

8.1.1.2.Data subject

The data subject is generally defined as the person to whom the personal data relate.

8.1.1.3.Personal data processing[33]

The concept of processing is very broad. It covers any operation or set of operations that are performed upon personal data, whether or not by automatic means.

In this frame, data processing is considered to be the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.

The data protection legislation covers both automated processing and non-automated processing. However, non-automated processing operations need to form part of a filing system or to be intended to form part of a filing system to be covered by the data protection legislation, i.e. *"any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis"* [34].

[33] Directive 95/46/CE, art. 2(b).
[34] Directive 95/46/CE, art. 2(c).

According to the Working Party on the Protection of Individuals with regard to the Processing of Personal data (also called 'Article 29 Working Group'), the concept of processing also includes the operations performed on Internet by software and hardware, such as the uses of cookies, the data subjects being unaware of these operations[35].

8.1.1.4.Controller and processor

According to Article 2(d) of the Directive, the controller is the natural or legal person (a company) who alone, or jointly with others, determines the purposes and the means of the processing of personal data. In every case, it is important to identify the data controller since he is the one liable for the legality of the processing. He also has to fulfil obligations towards his national data protection authority and towards the data subjects.

On the other hand, according to article 2(e) of the Directive, the processor is the natural or legal person, public authority, agency or any other body who processes personal data on behalf of the controller.

This will typically be a specialized third-party company entrusted by the controller to conduct the technical aspects of

[35] Recommendation 1/99 on Invisible and Automatic Processing of Personal data on the Internet performed by Software and Hardware adopted by the Working Party 16 on 23 February 1999.

the processing, such as the sorting or the combination of personal data.

The employee of the controller in charge of the security and of the management of the computer system is not to be considered as a processor.

8.1.2.Part I: B: Scope and Principles of the Directive

8.1.2.1.Scope of the Directive

According to the European Directive as well as to Convention No. 108 of the Council of Europe mentioned above, data protection principles apply to public and to private sectors.

As explained here above, the Directive 95/46/CE applies to the processing of personal data wholly or partly realised by automatic means, and to the processing realised by non automatic means when the personal data processed form part of a filing system or are intended to form part of a filing system[36].

8.1.2.2.Relevant principles for medical data processing of the Directive

One of the main principles of the Directive relies on the conviction that the risk of infringement of a data subject's rights and freedoms does not depend on the information contained in his data. This risk depends on the purpose of the processing of these personal data. In other words, the potential or actual danger for the data subject's fundamental rights and freedoms has to be assessed regarding the purpose of the processing of personal data. The purpose refers to the general aim and framework of use of the personal data.

The principle is slightly -though not entirely- different for special categories of data such as sensitive data or medical

[36] Directive 95/46/CE, art. 3.

data. Indeed, it is commonly admitted that the sole content of these data already exposes the data subject to the risk of infringement of his fundamental rights and freedoms, whatever the purpose of the data processing could be.

Therefore sensitive data require a special protection taking into account their content and the purpose of their processing.

For this reason, and as stated in the Recital 33 of the Directive, *"data which are capable by their nature of infringing fundamental freedoms or privacy should normally not be processed […]"*.

The Directive thus banishes the processing of sensitive or medical data, in order to ensure the respect of the data subject's fundamental rights and freedoms regarding the processing of his medical data.

However, the principle of the ban on the processing of sensitive and medical data is not absolute, as the full text of Recital 33 of the Directive states that *"data which are capable by their nature of infringing fundamental freedoms or privacy should normally not be processed unless the data subject gives his explicit consent […]"*.

The data subject's explicit and valid consent[37] thus constitutes the very first source of the legitimacy of the processing of his medical data even if, at the same time, it is the weakest base to legitimate the processing of medical data due to the strict conditions for its validity and to the possibility for the data subject to revoke his consent to the processing of his medical data at any time and without justification (as will be explained below)[38].

[37] Directive 95/46/CE, art 8, 2(a).

[38] As stated by senior researcher Jean Herveg, this empowerment of the data subject could surprise. One could indeed have doubts regarding the data subject's capacity to consent, in a reasonable way, to the processing of his or her medical data, at a time when he or she is the weakest person in his or her relation to the health practitioner or at least the demanding party in the processing of his or her medical data. See HERVEG, J., "The Ban on Processing Medical Data in European Law: Consent and

Nevertheless the Directive grants permission to process medical data in six other hypotheses.

Article 8, 2 of the Directive prescribes that:

"Paragraph 1 (i.e. the ban on the processing of medical data) *shall not apply where:*
[…]
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person when the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims".

The processing of medical data is equally permitted when it *"[…] is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and when those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy"* [39].

Alternative Solutions to Legitimate Processing of Medical Data in Healthgrid", *op.cit.*

Finally, the European Directive offers the opportunity to the Member States to add exemptions to those listed above, for reasons of substantial public interest. These exemptions should be subject to suitable safeguards. For instance, under Article 8, 4 of the Directive, national exemptions might be adopted for scientific research or for social security reasons.

In the cases listed in Article 8, paragraphs 2, 3 and 4 of the Directive, the legitimacy of the processing of medical data is formally presumed. This presumption has been settled down because the situations described in the hypotheses listed above justify the processing of medical data. The legitimacy of the processing of medical data is formally presumed, but without prejudice of the other conditions ensuring the lawfulness of the data processing.

8.1.3.Part I: C: The Lawfulness of the Data Processing

As regards medical data processing under the exceptions listed in Article 8 of the Directive, the other conditions ensuring the lawfulness of the data processing still apply.

Indeed, Article 8 of the Directive is part of Chapter II of the text named “General rules on the lawfulness of the processing of personal data”, which also contains other provisions concerning the lawfulness of the processing of personal data.

In other words, one could see Chapter II of the European Directive as a big concentric circle. Article 8 of the Directive,

[39] Directive 95/46/CE, art. 8, 3. See also Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, which foresees the same thing as the article 8, 3 of the Directive.

which relates to the processing of special categories of data (for instance medical data subject to a higher level of protection), would then be a smaller concentric circle included in the first one.

It is thus logical that all the conditions of the first concentric circle listed below apply to the smallest concentric circle.

A single exception in this reasoning: Article 8 of the Directive darkens Article 7. To be qualified as legitimate, the processing of medical data does not have to correspond to one of the social justifications laid down by the European Directive in its Article 7. It just has to correspond to one of the seven hypotheses listed in Article 8 of the Directive mentioned here above.

8.1.3.1.Conditions regarding the quality of the personal data

As provided for in Article 6 of the Directive, when a data controller needs to process specific data, these data must meet a certain level of quality and thus have to comply with different principles.

8.1.3.1.1.Personal data must be processed fairly and lawfully[40]

[40] Directive 95/46/CE, art. 6, 1(a).

> The controller may process personal data only if such processing is done in accordance with the relevant legislation and complies with good practices.

To be lawful, the processing must comply with the data protection legislations at European and national levels. It must also comply with other legal requirements (for instance, special legal texts relating to the medical sector, such as texts or recommendation dedicated to medical secrecy).

To be fair, the processing must be transparent to the data subject. This means that the controller has to comply with his information duty (as we will see below) and to respect principles of good practices that should be listed in Codes of conduct.

8.1.3.1.2. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards[41]

In order to grant a certain quality to personal data collected, the data controller has to define precisely the purpose of the

[41] Directive 95/46/CE, art. 6, 1(b).

processing he plans to do and to communicate it to the data subject and to his national supervisory authority.

Each purpose must be legitimate, meaning that the interest of processing must outweigh the data subject's interests in not having his data processed. In this framework one has to underline that the Directive's text provides hypotheses where the legitimacy of the data processing is presumed. But even in those hypotheses, the legitimacy has to be assessed *a posteriori* and a balance of interests has to be established.

For example the data processing could be legitimate if it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except when such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

To rely on this justification, the data controller should at first identify the interests being pursued by the processing. He would then have to determine whether these interests are legitimate (they must at least not violate any legal provision). Finally he would have to verify that the data processing does not impact the data subject's rights and liberties in a

disproportionate way. The data subject's rights and liberties should indeed prevail over the data controller's interests.

In order to assess the existence of prevalence, the controller takes into account the data subject's interest in not having his data processed and any potential damage or distress that could be caused to the data subject by the processing of his data. Moreover, when the purpose of the processing can be achieved by different schemas of processing, the controller should always prefer the one lesser damaging or inconvenient for the data subject.

The data collected may only be used for the initial purpose of the processing and should not be re-used for an incompatible purpose. When the data controller intends a new processing of the data, the purpose of this new processing has to be compared with the initial one in order to assess whether there is a close relationship between both. A new purpose that is clearly different from the initial one is to be considered as incompatible with the first one.

When assessing whether the new purpose is compatible with the initial purpose of the processing, the data controller shall have regard to the context, the general philosophy of the

second processing, as well as to any other relevant criteria as whether or not the secondary processing will be conducted by a third party or as whether the applicable law authorizes a second processing or not.

However, a presumption of compatibility with the initial purpose of the processing applies to further processing for historical, statistical or scientific purposes. Those purposes are considered compatible with the purpose for which the data had originally been collected, provided that the data controller respects the specific safeguards foreseen by each Member State. Therefore, it would be possible for the data controller to re-use data if the purpose of a second processing is scientific or statistical despite that it totally differs from the initial purpose of the processing. In this framework, the data controller must rely on the applicable national legislation in order to determine the conditions and how to comply with them.

8.1.3.1.3. Personal data must be adequate and relevant and may not be excessive.[42]

Personal data must furthermore be useful and relevant as regards the declared purpose of the processing. It is

[42] Directive 95/46/CE, art. 6, 1(c).

thus forbidden to collect or to make use of irrelevant data that are not pertinent or not necessary to achieve the purpose of the processing. The data controller should therefore avoid the use of personal data when the purpose of the planned processing can be achieved without it.

On the other hand, the data collected may not be excessive. This means that collecting certain data should not create a disproportionate risk of undermining data subject's interests. In this framework, useful data that are thought not indispensable to achieve the purpose of a processing have to be considered as excessive.

8.1.3.1.4. Personal data must be accurate and, when necessary, kept up to date.[43]

Another important matter to ensure the quality of the data is the accuracy of the processed data. To keep the data accurate and when necessary up to date is an obligation of the data controller. He thus has to take all reasonable measures to fulfil his duty. He must prevent

[43] Directive 95/46/CE, art. 6, 1(d).

from processing erroneous, incomplete or obsolete data.

Moreover, when he knows that the data collected and processed are not accurate, he must either erase or rectify them.

8.1.3.1.5. Personal data should be stored for a limited period of time.[44]

The quality of the data is ensured by a last obligation lying on the data controller. Indeed personal data must not be kept in a form that permits the identification of the data subject for longer than what is necessary for the purposes for which they were collected or for which they are further processed.

As soon as the purpose of the processing can be achieved without using personal data, there is no need to conserve such data any longer. Therefore, they should be rendered anonymous[45] or be destroyed.

The Directive authorises the Member States to allow the data storage for a longer period of time, provided that the long-term

[44] Directive 95/46/CE, art. 6, 1(e).

[45] For a detail analysis on anonyms data and how to render a data anonymous in compliance with Directive 95/46/CE, please consult the reports to be published in the framework of the ACGT Project.

storage aims at using the data exclusively to carry out scientific research or statistics. Most Member States have transposed this provision of the Directive and their legislations provide for a special authorisation for long-term storage.

Recommendation R (97) 5 of the Committee of Ministers to Member States of the Council of Europe on the protection of medical data adopted on 13 February 1997, also authorises longer-term storage for interest of public health or in order to enable the controller to defend or exercise a legal claim. When a longer-term storage is rendered possible, security measures should be taken to ensure the correct conservation of the data[46].

8.1.3.2.Conditions regarding the rights of the data subject

Certain rights are granted to data subjects with regard to the processing of their data: a right of information, a right of access to their personal data, a right to request correction of the data and a right to object to the processing of the data under specific circumstances. The fact that these rights are recognised to data subjects helps to protect their rights of privacy and their fundamental liberties in more effective way. Furthermore, so, data subjects do not feel totally dispossessed of information that concerns them. When these conditions are not respected, the processing of personal data should be seen as unfair in respect of data subjects. The controller should therefore anticipate the likely exercising of these rights[47].

[46] See Chapter II of this document.

[47] The exercising of these rights specially requires the data controller to take the technical measures that would be dealt with in the second Chapter (II) of this document.

8.1.3.2.1.Right to be informed

Personal data can either be obtained directly from the data subject (which is called the *'primary collection'*) or be obtained from a distinct alternative source of data, as a hospital or a doctor (which is called the *'secondary collection'*).

The information to be given to the data subject is governed by Article 10 of the European Directive in case of *primary collection* and by Article 11 in case of *secondary collection*.

8.1.3.2.1.1.Primary collection

Primary collection covers all situations where the personal data are collected directly from the data subject, including those where the data subject ignores or is unaware of the fact that personal data are collected.

In this case, the controller or his representative (if any) must provide the data subject specific information relating to the processing. In order to protect his rights, the data subject must indeed learn about the existence of a processing operation on his data[48].

The controller will thus have to provide at least his identity (name, address, denomination or trade name, etc.) and his representative's name (if any)[49].

He will also have to provide a description of the purposes of the processing. These purposes have to be specified and explicit, which means that the precise description of the scientific or the statistical project is to be given. The aim of this information obligation is to indicate what the data will be used for. To inform the data subject that the data will be used for a scientific

[48] The information duty does thus not apply where the data subject has already been informed or when he already knows about the data processing.

[49] Directive 95/46/CE, art. 10(a) and art. 11, 1(a).

or for a statistical purpose is thus not enough. The data subject must have an accurate idea of what the research or the statistics planned by the data controller will be about.

The controller has to provide the data subject with additional information. When it is necessary to guarantee the fairness of the processing, this additional information would be for example information about the categories of data concerned by the processing, about the recipients or the categories of recipients of the data, about the existence of a data subject's right of access to his data or about the existence of a data subject's right to rectify his data.

The processing of sensitive data or medical data normally requires the provision of further information. For instance, in case of genetic analysis, the data subject should be informed about the objectives of the analysis and about the possibility of unexpected findings[50].

Finally as what regards the timing of the provision of the information, it should be given to the data subject at the same time when the data are collected, at the latest. However, when

[50] See Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data adopted on 13 February 1997.

medical data are collected for medical emergencies, data necessary for the medical treatment may be collected at first.

In case of genetic analysis, the information should be given to the data subject before the genetic analysis is carried out.

8.1.3.2.1.2.Secondary collection

When personal data have not been obtained directly from the data subject, the controller should, before considering the way of processing these personal data or the right time to inform the data subject, assess whether they comply with the requirements for re-use of data[51].

The controller has to inform data subjects about any secondary collection at the latest at the time of recording, or if disclosure to a third party is anticipated, no later than the time when the data are first disclosed.

The duty of information does not apply where in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such

[51] See paragraph 2.2. supra.

information proves to be impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. Disproportionate effort may result when it is impossible to reach or contact data subjects (for example when the controller cannot easily obtain their addresses) or when contacting all data subjects can only be done at great expense, which is disproportionate in comparison with the risk of infringing their rights.

8.1.3.2.2.Right to access the data [52]

All data subjects have the right to request specific information about their own personal data that are processed by the controller. Moreover, where medical data are processed, data subjects may ask a healthcare professional to exercise their access right.

Upon request, the controller will have to provide the data subjects with information such as whether or not he his

[52] Directive 95/46/CE, art. 12(a).

processing data relating to them. He will also have to inform them about the purpose of the processing, the categories of data and the data being processed, the recipients or categories of recipients to whom the data are disclosed and the source of the data.

The Directive allows Member States to exempt the controller from respecting the data subject's access right where the purpose of the processing is scientific research, or when data are kept in personal form for a period which does not exceed the period necessary to create statistics.

The Directive, however, subjects the granting of that exemption to the condition that there is clearly no risk of breach of the data subject's privacy. Moreover, data may not be used in order to take measures or decisions regarding any particular individual.

8.1.3.2.3.Right to rectify the data

Under the Directive, a data subject has the right to ask for data to be corrected, erased or blocked where their processing does not comply with the provisions of the Directive[53]. This is particularly the case where personal data are incomplete or inaccurate.

This right means that the controller must correct, erase or block the data as required by the data subject, in a reasonable period.

Blocked data cannot further be processed, used, or communicated without the data subject's consent.

In addition, if the controller has disclosed the data to third parties, he has to notify them about any correction, erasure or blocking carried out. This notification of correction, erasure or

[53] Directive 95/46/CE, art. 12(b).

blocking of data does not have to be performed if it proves to be impossible or involves a disproportionate effort[54].

The Directive allows Member States to exempt the controller from the obligation to respect the data subject's right of correction in case of processing for purposes of scientific research, or when data are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics[55].

8.1.3.2.4.Right to object to the processing

The last right granted to the data subject is the right to object to the processing of his data. When there is a legitimate objection to the data processing, the controller may no longer process the concerned data or communicate them to recipients.

According to the Recommendation No. R (83) 10 of the Committee of Ministers to Member States on the protection of personal data used for scientific research and statistics, adopted on 23 September 1983, where processing is conducted

[54] Directive 95/46/CE, art. 12 (c).
[55] Directive 95/46/CE, art. 13, 2.

for scientific or statistical reasons, the data subject may withdraw his collaboration. It this hypothesis, the data subject is entitled to ask the erasure of the data collected from him.

8.1.3.3.Duties of the controller[56]

The controller has the obligation to ensure the security of the personal data processed, meaning that he must ensure that the data collected and stored are not lost, altered or accidentally destroyed.

These duties of the data controllers will be analysed in the second Chapter of this Part of the document devoted to the network components of the grid technology.

8.1.4.Part I: D: Transfer of Personal Data between Member States: the Impact of National Legislations

The transfer of personal data between two or several controllers established on the territory of one Member States or

[56] Directive 95/46/CE, Section VIII 'Confidentiality and Security of processing'.

on the territories of several Member States involves on one hand a problem of communication of personal data to third parties and on the other hand a problem of transfer of personal data.

8.1.4.1.Communication of personal data to third parties

As regards the transfer of personal data between different controllers established on the territory of one Member State or on the territories of different Member States, the first problem to be solved lies in the general principle according to which controllers should refrain from communicating or publishing personal data or otherwise making them public when it is not necessary to achieve the purpose of the processing.

Indeed, the transfer or the disclosure of personal data to third parties is considered as a processing operation and, as such, it is subject to the processing legal requirements.

In this framework, as explained above, the controller should check whether or not the transfer or disclosure of personal data falls within the scope of the initial purpose of the processing or is still compatible with this purpose, in order to determine whether or not he can transfer or disclose the personal data concerned.

The only data that can be transferred without being subject to these specific requirements are anonymous data.

Finally, it is important to underline that the transfer of medical data is subject to additional specific requirements.

Medical data should not be communicated unless the conditions listed hereunder are fulfilled:

- medical data to be communicated are relevant for the communication purpose;
- the recipient of the communication is subject to confidentiality rules equivalent to those incumbent to healthcare professionals, and the communication is legally authorised and is realised for public health reasons or for another important public interest, to prevent a real danger or suppress a specific criminal offence, to protect the rights and freedoms of others or of the data subject himself or of a relative in genetic line, to safeguard the data subject's vital interests or a third person's ones, to fulfil specific contractual

obligations or finally to establish, exercise or defend a legal claim.

Medical data can also be communicated if the first condition here above is met (i.e. data to be communicated are relevant for the communication purpose) and if the data subject (or his legal representative (if any) or an authority) has given his consent to the communication.

Last but not least, medical data relevant for the communication purpose may be communicated if the concerned data subject (or his legal representative (if any) or an authority) has not explicitly objected to any non-mandatory communication, if data have been collected in a freely chosen preventive, diagnostic or

therapeutic context, and if the purpose of the communication, in particular the provision of care to the patient, or the management of a medical service operating in the patient's interest, is not incompatible with the purpose of the initial processing.

But the communication of medical data between EU Member States also raises a problem of data transfer between different countries, as the data protection national legislations are not fully harmonized.

8.1.4.2.Transfer of personal data between EU Member States

Under Article 32, 1, first paragraph of the European Directive, *"Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive […]".*

National legislations of the different EU Member States should be harmonised by now, and the transfers of personal data between these Member States should not create any problem.

For instance, a data controller established on the territory of one Member State should not fear by transferring the data he processed to another controller established in another Member State, that these data would not be correctly protected as the second Member State does not provide for the same level of protection of personal data as the first one.

This would be the case if all Member States had transposed the Directive in the same way.

But differences are already to be found in the member States' legislations as regards the definitions of key concepts of the Directive such as 'personal data', 'processing' or 'controller'.

Moreover, the Directive itself allows the Member States to *"adopt legislative measures to restrict the scope of the*

obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitute a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(a)[…]".

There might thus be differences in the level of protection granted to personal data between the EU Member States, which

might be a problem for the implementation of the healthgrid technology on the whole territory of the European Union.

However, it is important to note that even if there are differences in the levels of protection of personal data between the Member States, these differences are of minor importance, as the implementation of the Directive already ensures a high level of protection for personal data. These differences in the levels of protection of personal data between the Member

States cannot even constitute barriers to data transfers as Article 1, paragraph 2 of the Directive prescribes:

"Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1 (i.e. the protection of data subjects' fundamental rights and freedoms)*".*

This is not always the case as what regards the transfer of personal data towards other countries located outside the European Union and the European Economic Area (EEA).

8.1.5. Part I: E: Transfer of Personal Data to Non-EU (and Non-EEA) Countries

The transfer of personal data outside the European Economic Area is governed by specific conditions[57] that need to be met in addition to the requirements for the communication of personal data to third parties analysed in point D, 1., here above.

The controller should refrain from transferring personal data to a recipient located in non-EEA countries, if the country involved does not ensure an adequate level of protection.

Some countries, such as Argentina, Isle of Man, Guernsey and Switzerland, have been recognised by the European Commission as ensuring an adequate level of protection. This means that the European Commission has decided that these countries have a level of protection of personal data in some way equivalent to the one available in the Member States of the European Union.

The transfer of data to companies located on the territory of the United States, which adhered to the US Department of Commerce's Safe Harbour Privacy Principles, is also allowed.

[57] Directive 95/46/CE, articles 25 and 26. The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26 (4) of Directive 95/46/EC that certain standard contractual clauses offer sufficient safeguards as required by Article 26 (2), that is, they provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.
The effect of such a decision is that by incorporating the standard contractual clauses into a contract, personal data can flow from a data controller established in any of the Member States of the EU and in the three EEA member countries (Norway, Liechtenstein and Iceland) to a data controller established in a country not ensuring an adequate level of data protection. Moreover on the 15 June 2001, the Commission adopted Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries. Recently, i.e. on 27 December 2006, the Commission adopted Decision C(2004)5271 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, *O.J.,* L 385/74, 29 December 2004.

The European Commission moreover allows the transfer of personal data to recipients located on the territory of Canada, provided that these recipients are subject to the Canadian Personal Information Protection and Electronic Documents Act (also called the 'PIPED Act'). However, the PIPED Act mainly addresses organisations that are regulated at a federal level (federal works, undertakings or businesses) and not non-profit organisations.

Regarding the other countries, it is up to the controller to assess whether or not they offer an adequate level of protection of personal data.

The controller can find all the same a loophole in the Directive. Indeed the Directive provides some exemptions to the prohibition of transfer of personal data to countries not offering an adequate level of protection of personal data.

The most relevant exemptions contained in most of the national laws with respect to processing for research and statistical purposes are the following:

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or

the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case[58].

Moreover, the Directive states that Member States may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection of personal data, where the controller adduces adequate safeguards as what regards the protection of the privacy, fundamental rights and freedoms of individuals and the exercise of the corresponding rights. Such safeguards may result, in particular, from appropriate contractual clauses[59].

The European Commission decided that an adequate level of protection of personal data could, in particular, be achieved through a contract between the sender and the recipient of the personal data. In this frame, the European Commission proposes standard contractual clauses that ensure an adequate level of protection of transferred personal data.

The European Directive does not set specific conditions for the transfer of medical data to non-EU (and non EEA) countries, but Recommendation R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, does so. It establishes additional rules for the transfer of medical data to a country that does not have an equivalent level of protection of medical data as the one granted on the territory of the European Union.

[58] Directive 95/46/CE, art. 26, 1(a) to (f).
[59] Directive 95/46/CE, art. 26, 2.

Under these circumstances, the person responsible for the data transfer should indicate to the recipient the initial purpose of the processing as well as the persons or the bodies to whom the data may be communicated.

On the other hand, the recipient should honour the purpose he accepted and should not communicate the data to other persons or other bodies than those indicated by the person responsible for the data transfer.

8.1.6. Part I: F: Additional Specific Rules for the Processing of Medical and Genetic Data

The European Directive does not contain all the rules relating to the processing of medical or genetic data.

Some specific rules relating to the processing of medical data have been proposed by the Council of Europe within Recommendation R (97) 5 of the Committee of Ministers to

Member States on the protection of medical data, adopted on 13 February 1997.

As provided by this Recommendation, only healthcare professionals or individuals or bodies working on behalf of those healthcare professionals should carry out the processing of medical data. Those individuals or bodies should be subject to confidentiality rules equivalent to those incumbent on healthcare professionals[60].

[60] This requirement is equivalent to the one contained in Article 8, 3 of the European Directive which provides that *'Paragraph 1 shall not apply where processing of data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*".

Moreover medical data must normally be obtained directly from the data subject, but it is possible to obtain such data from other sources of information when some conditions are met (as provided for in the Directive).

Finally, medical data should not be communicated to third parties unless some conditions are met.

As regards the processing of genetic data, the Recommendation No. R (97) 5 establishes specific rules. In the framework of the

Recommendation, genetic data collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research, should only be used for those purposes or in order to allow the data subject to take a free and informed decision on the opportunity of such treatments or researches.

On the other hand, the collection and processing of genetic data should, in principle be permitted only for health reasons and in particular it should be authorised to avoid that any serious prejudice would be caused to the health of data subjects or

third parties. The collection and processing of genetic data may though be authorised in order to predict illness in cases of overriding interests. In this case, both operations will be subject to appropriate safeguards defined by the applicable legislation.

It is also important to underline that other specific rules exist for the processing of other person identifying data, when the purpose of the processing is scientific or statistical.

Recommendation R (83) 10 of the Committee of Ministers to Member States on the protection of personal data used for

scientific research and statistics, adopted on 23 September 1983, proposes different principles for the processing of these data for research or statistics purposes.

When it is possible, the researches should be undertaken with anonymous data. However, if using anonymous data renders the research impossible, personal data may be used. Under the circumstances that health data are use to achieve scientific researches, specific conditions listed by the Recommendation No. R (97) 5 must be met.

Indeed, personal data may not be used for another purpose than the one of the research itself, nor be used to take a decision or

to undertake any action directly affecting the data subject, nor be used for another research project substantially different in its nature or in its objects from the initial one, except if the data subject gave his consent.

The personal data may not be published unless the data subject has consented to the publication and under the circumstances that the national law allows it.

8.2. PART II: NETWORK COMPLIANCE WITH CONFIDENTIALITY AND SECURITY REQUIREMENTS

As said in the Part I of the analysis, personal data processing has consequences, for example as regards the data subjects' rights. When their data are processed, the law recognises them certain rights. In this framework, the data controller should anticipate the likely exercising of these rights by adapting his system.

The networks hosting data processing are thus to be adapted to it and to be adapted to all the consequences in terms of

confidentiality and security (Part II B) and in terms of notification duty (Part II C).

On the other hand, as stated by Professor Yves Poullet, the creation of new telematic infrastructures raises the question about the person (natural or legal person) responsible for the infrastructure[61]. The answer to this question should not be neglected, as the "network controller" would be responsible for the conception and the quality of the network.

[61] HERVEG, J. and POULLET, Y., *Which major legal concerns in future e-Health?,* e-Health and Health Policies, Synergies for better health in a Europe of Regions, Plenary session: e-health and new social dilemmas, to be published. JH comments that this paper has been published: details needed.

8.2.1.Part II: A: Confidentiality and Security Issues

Data processing confidentiality and security requirements are mainly regulated by Directive 95/46/CE. The 8th section of the European Directive is dedicated to these issues.

As what regards the confidentiality necessarily linked with the data processing, Article 16 of the Directive provides that *"any person acting under the authority of the controller or of the processor including the processor himself, who has access to*

personal data must not process them except on instructions from he controller, unless he is required to do so by law".

The controller must ensure the confidentiality of the personal data, meaning that unauthorised access to them or disclosure must be prevented.

On the other hand, Article 17 of the Directive governs the security of the processing.

According to Article 17 of the Directive, the controller has the obligation to ensure the security of the personal data processed,

meaning that he must ensure that the data are not lost, altered, or accidentally destroyed.

As said before, the controller must also ensure the confidentiality of the personal data processed.

In order to achieve those two purposes, the controller must implement appropriate technical and organisational measures to protect personal data against, for instance, accidental or unlawful destruction or accidental loss, alteration, unauthorised

disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing[62]. In other words, the controller has to construct his system to render it sufficiently secure for the processing of personal data.

As well, he might have to adapt the organisational structure of his company to ensure the confidentiality and the security of the data processed[63].

This means that the protection of the data enclosed in the system has an impact on the system itself. The data controller

[62] Directive 95/46/CE, art. 17, 1, § 1.

[63] An example of an organisational measure could be the appointment of a data protection officer in charge of the data protection issues. On the other hand, technical measures could include restricted access to the databases to authorized persons and the utilisation of software protecting the system against viruses or hacking.

must collaborate with the network controller to fulfil the confidentiality and security requirements. The infrastructure must be confidential to protect patients' rights. It must also be secure and stable to prevent any damage to the data collected, processed and stored.

According to the law[64], the appropriate level of protection to ensure depends of the state of the art, the cost of the system implementation, the sensitisation and the staff training in data processing, the risks represented by the processing, and the nature of the data to be protected (for instance sensitive data like health data require a higher level of protection).

Recommendation R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, gives some example of the measures that could be taken when medical data are processed. The data controller and the system controller could, following the examples given in the Recommendation, control the entrance to their installations (by using a password), to prevent any unauthorised person to have access to the data.

Moreover, both controllers should appoint a person responsible for the security of the information system and for the data protection.

It can also happen that the controller will not be the one processing the data, but that he would appoint another person (named the 'processor') to process the data on his behalf. Article 17, 2 of the European Directive, regulates this hypothesis.

Under these circumstances, the data controller must take reinforced security and confidentiality measures because the information he collected are transferred to another person who will process it. He should then ensure that the processor

[64] Directive 95/46/CE, art. 17, 1, § 2.

provides sufficient guarantees on technical security measures and on organisational measures governing the processing to be carried out and on the fact that he will comply with those measures.

Moreover in this case the European Directive requires the data processing to be governed by a contract or by a legal act binding the processor to the controller and stipulating in particular that the processor shall only act on the instructions

of the controller and that he should be responsible for taking all appropriate technical and organizational measures.

In view of keeping proof, the parts of the contract or of the legal act binding the processor and relating to the data protection shall be in written form or in another equivalent form[65].

For technicians, it may seem difficult to comply with the confidentiality and the security constraints, especially as they are actors non subject to medical deontology or medical

[65] Directive 95/46/CE, art. 17, 4.

secrecy. In a general way, the creation and the implementation of healthgrids in the healthcare sector in particular may be in conflict with traditional rules relative to medical secrecy. However, information society technologies may provide many solutions to these problems[66].

8.2.2.Part II: B: Notification Duty

In order to ensure some kind of publicity and transparency around the existence and scope of any processing, the controller is required, prior to carrying out the processing, to

[66] Directive 2002/58/EC provides, in its Articles 4, 5, 6 and 9, rules concerning the security and the confidentiality of electronic communications but unfortunately only for infrastructures open to the public and accessible to him.

provide the relevant national supervisory authority with certain pieces of information regarding the processing he is planning to conduct. The information recorded will then normally be accessible to data subjects or to third parties.

This does not really concern the network or the system with which the processing will be undertaken, but it requires the system to satisfy to the confidentiality and security legal requirements, as the national supervisory authority will be

aware of its existence and will be able to check whether or not it satisfies to the legal requirements.

The notification will notably cover the identity of the controller, the purpose of the processing, the categories of data subjects, the recipients, and the transfers to third countries.

However, the exact content of the notification has to be defined by the different national laws and further specified by National Data Protection Authorities.

9. ANNEX II: LIABILITY ISSUES

As we saw in the Annex I, implementing a healthgrid generally implies the processing of patients' personal health data, which implies risks for patients' rights and liberties.

Implementing a healthgrid and using it in a hospital for instance, implies other risks for patients. Indeed in case of malfunctioning of the system or of problem in the supply of services, patients could be harmed.

The issue in the case of damages caused to patients by a malfunctioning of the system or by a product or service part of the system, is that there are currently no specific guidelines or liability rules available to solve potential problems.

Originally, the medical liability issue appeared in the relationship between a patient and a healthcare practitioner (usually a doctor). Thus, when a patient was victim of medical negligence or of a medical error, the solution would be quite

simple: he would take legal action against his doctor or prosecute him.

Quickly, a new actor appeared within the framework of the treatment of diseases and illnesses, in the event of error or of negligence of the healthcare practitioner, namely the insurance company of the healthcare practitioner.

Determining the responsibilities for each one became even more difficult, when the patient was taken in charge by a

medical team or by different healthcare practitioners members of a hospital service. Who should be regarded as liable in the event of problems? The doctor? All the members of the medical team in charge of the patient? The hospital?

New questions arise as the complexity of the relations between patients and doctors increases: What is the responsibility of the doctor delivering a second opinion, in case of accident? What is the patient's responsibility in the damage that was caused to him? What about the State's liability, i.e. in the organisation and

the monitoring of the health activities? What could be the responsibility of the pharmaceutical companies in issuing dangerous medicinal products when those products were prescribed by doctors?

Nowadays, the implementation of healthgrids notably in the healthcare sector introduces even more difficulties in the determination of responsibilities in case of damage cause to a patient.

Even if at first the medical liability has to be considered in the relationship between the patient and the healthcare practitioner,[67] the establishment of the person to be hold responsible for a specific damage can be problematic taking into account the number of intermediaries participating to a healthgrid and the complexity of such a system involving different actors such as doctors, specialists, hospitals, pharmaceutical companies, data controllers and processors, technicians, etc., often located in different countries.[68]

Although there are no specific liability rules applicable to products and to services that are supplied by the healthgrid systems or that compose them, a general principle exists that products and services provided to consumers must comply with certain level of quality.[69]

[67] The principle is that a patient victim of a medical negligence or error will at first bring proceedings against his doctor. The generalist is thus the front line in case of medical damages caused to a patient.

[68] As stated by senior researcher Jean HERVEG in the report *Product Liability and Consumer Protection* (to be published in the context of the INFSO financed study "Legally eHealth"), in the healthcare practice, the patient is nowadays frequently aware of the different intermediaries in charge of his file. In case of damage, he could then logically bring proceedings against them rather than against his doctor. Difficulties could then occur from the differences in the way their responsibility is been engaged. On the other hand, the patient is more and more in charge of his health, without the intervention of a healthcare practitioner. Thus, beyond the articulation of the different healthcare practitioners' liability, there are situations where the patient is no more taken in charge by a healthcare practitioner. Under these circumstances, the patient stands alone against the pharmaceutical companies or the medical devices companies which might be subject of different rules regulating their liability. It might thus be impossible for the patient to find an interlocutor and to obtain compensation for the damage caused to him. JH proposes to delete this note – need explanation.

[69] This principle applies mutatis mutandis to business-to-business relations. See Chapter II: Liability as regards the system's components of this document infra.

At European level, different legislations have been adopted in order to protect consumers. These legislations provide consumers with a legal guarantee of high level quality products and services. They also contain provisions dedicated to the redress of damages resulting from sub-standard products or services.

Even if these texts are not directly dedicated to products and to services supplied by healthgrid systems or elements composing them, they can be easily applied there.

At first, we shall thus analyse the European legislation applicable to the information contained in the healthgrid systems or to the products and the services supplied by these systems (Part I). We shall approach then the useful texts to determine the responsibilities of the different actors of healthgrids, as for the elements that compose these systems (Part II). Finally, we will detail some situations, as the fact that a pharmaceutical product is sold by Internet or that a contract is concluded electrically, in which the particular responsibility of certain actors of the system is determined well (Part III).

9.1. LIABILITY AS REGARDS THE SYSTEM'S CONTENT

As stated in the first part of this document, healthgrids mainly contain patients' medical data, such as personal data, insurance data, medical images, radiographies, results of blood tests or others, domestic antecedents, etc.[70] These data when processed constitute a risk for patients' fundamental rights and freedoms. Someone would thus be hold liable if patients' medical data are destructed, lost, altered or disclosed to unauthorised third parties (Part I A).

healthgrids used in the drug discovery sector also contain information helping to develop new medicinal products. For instance, a foreseeable future is to enable a complete in silico drug discovery pipeline on the grid. Such pipeline would allow very quickly identifying promising compounds. But who would be responsible, if for example, a medicinal product developed with one of those new compounds is dangerous for human health. Who would be liable for the damages caused to patients' health (Part I B)?

Finally products and services are offered to healthcare practitioners and patients through healthgrid systems. Indeed, if a doctor refers the case of his patient to colleagues in another hospital and if these colleagues come up with a diagnosis, one can say that a service has been provided through a grid. But what if this diagnosis is wrong and the patient die or if the diagnosis is not provided on time to the doctor. Who would be responsible for the damage causes to patient and to his family (Part I C)?

9.1.1.Part I: A: Liability as regards the Data

As stated in the first part of this document, processing of personal data requires security and confidentiality of information highways. These requirements

[70] When a healthgrid is use in the biomedical sciences, in the life science, in the medical research or in the drug discovery sectors, it contains wealth data, molecular biology data or medical images.

encompass both levels of the information system. To ensure the confidentiality and the security of the data processing performed in the framework of the second level of the information system, the infrastructure (which constitutes the first level of the information system) must be secure and stable.

In terms of confidentiality, this implies that any person acting under the authority of the data controller or of the data processor, including the data processor himself, who has access to personal data, must not process them except on instructions from the controller.[71]

[71] Directive 95/46/EC, art. 16.

In terms of security, this implies that the data controller in due cooperation with the network controller must implement appropriate technical and organisational measures to protect personal data.

There are thus three important actors, the data controller, the data processor and the network controller, who have to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, etc.

Tough if one of these incidents happens, it would be difficult for the patient to determine to whom he might ask compensation for the damage caused to him.

Directive 95/46/CE prescribed that every person has the right to a judicial remedy for any breach of the rights guaranteed by the national law applicable to the processing in question.[72]

Article 23, first paragraph of the Directive even stipulates that:

"Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered".

The data controller would then be liable in case of damage caused to a patient and he would be responsible to repair this damage.

However, he would be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.[73] He could for example prove that a default of maintenance of the system by the network controller gave raise to the patient's damage.

[72] Directive 95/46/EC, art. 22.
[73] Directive 95/46/EC, art. 23, § 2.

As regards data contained in healthgrid systems, the question of liability in case of damage is easily solved, thanks to the European Directive's prescriptions. This is not always the case.

9.1.2.Part I: B: Liability as regards Products

Diverse products might be delivered through healthgrid systems to patients, such as medicinal products, pharmaceutical products or any other kind of products use in relation with the patient's health.[74] Formulas can also be provided to different biomedical experts using the healthgrid. Yet, there is no specific definition of these products, as there is no specific legislation applicable to the liability deriving from the delivery and the use of these products.

However, the delivery and the use of these products may induce liabilities of persons active in the healthcare sector and treating patients through healthgrid systems, as healthcare practitioners, medical device producers,[75] pharmaceutical companies, hospitals, etc. They may also induce liabilities of actors of the biomedical sciences sector such as biomedical experts, or of the drug discovery sector.

To mitigate this deficiency, one might apply the general principles relative to consumers' protection.

The basic principle exists that if a product does not conform to the offer made or causes damages, the consumer (or another person representing him) may claim for compensation. Any liability issue will thus normally depend on the general rules of law applicable in the different EU Member States.

Though, there are some special European regulations applicable in case of damages caused to consumers by defective or not corresponding products.

[74] This is already the case at a London hospital where an ePharmacy has been set up through a combination of ePrescribing, eDispensing using a robot system, eStockmanagement and eProcurement, for outpatients and discharged patients.

[75] As regards the liability of these persons, see Chapter II of this document.

Among these texts, we distinguish those concerned the prevention (1) and those that allow to repair damages (2) or to have an appeal when the delivered product is not in accordance with what was foreseen in the contract (3).

9.1.2.1.Prevention

As we just said, certain European legislations permit to avoid that damages are caused to the consumers. To do it, these texts impose obligations, notably to the producers of products.

Texts applicable to products delivered by means of healthgrid systems are essentially Directive 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety (1.1.) and Directive 2001/83 of the

European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (1.2.).

9.1.2.1.1.Directive 2001/95 on general product safety[76]

Directive 2001/95 on general product safety imposes a general safety requirement for any product put on the market and intended for consumers or likely to be used by them.

[76] Directive 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety, *O.J. L11,* of 15 January 2002, 4-17.

Indeed, producers can put on the market only safe products which are not likely to cause any threat (or only a reduced threat in accordance with the nature of the product's use) and which allow an effective protection of the consumers' health and safety.

In addition, they must provide consumers with relevant information enabling them to assess the risks inherent to the product, particularly when these risks are not

obvious. They *must* also take appropriate actions to avoid these risks (withdrawal of unsafe products from the market, warning of the consumers, recall of unsafe products already supplied, etc.).

9.1.2.1.1.1.Some key concepts[77]

In the framework of Directive 2001/95, the term 'product' means any product which is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and which is supplied

[77] For a definition of all key concepts of the Directive and for a detailed analysis of the Directive's text see VEREECKEN, I. and HERVEG, J., *Product Liability and Consumer Protection,* Part II: Analysis of the relevant legal texts, (to be published in the context of the INFSO financed study "Legally eHealth").

or made available, whether for consideration or not, in the course of a commercial activity, and whether new, used or reconditioned.

Therefore, products initially reserved for professional use that are subsequently made available to consumers are also covered by the Directive's definition of the term product.

On the other hand, a safe product is any product which, under normal and reasonably foreseeable conditions of use including duration, does not present any risk or only minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection of consumers' safety and health.

A dangerous product does thus not meet the definition of 'safe product'.

9.1.2.1.1.2.Directive's scope

The Directive applies to any product insofar as no specific provision among the European Community legislations governing the product's safety is concerned or if sectoral legislation is sufficient.

The provision of services is excluded from the scope of the Directive, but the products supplied to consumers within the framework of the supply of a service are included in the Directive's scope.

9.1.2.1.1.3.General safety requirement

The basic principle included in the Directive is that producers are obliged to place only safe products on the market.

Some criteria are thus proposed in the Directive's text in order to assess if a product complies with the safety requirement. For instance, a product is deemed safe only once it conforms to the specific EU provisions governing products' safety.

Products producers and distributors also have their obligations, as mentioned above.[78]

9.1.2.1.1.4.Duty of the EU Member States

Member States have to established or designated national authorities in order to monitor the product safety and to take appropriate measures as regards risky products.

[78] For an overview of producers and distributor's obligations, see *Legally e-Health: Product Liability and Consumer Protection*, opcit.

Every national authority must ensure that producers and distributors comply with their duties and are entitled to ensure the product safety by organising checks on safety properties, by imposing producers to warn adequately on the possible risks, by prohibiting dangerous products to be marketed, by alerting consumers on the risks of a product already marketed and by organising recalls and destruction of products when necessary.

9.1.2.1.1.5.Information system

Directive 2001/95 aims to create an efficient information system in order to help EU Member States, national authorities and consumers to react quickly in order to avoid or to reduce any harm caused to persons' health and safety.

The producers and distributors who discover that a product is dangerous must notify the information to the competent national authority and collaborate with it.

The European Commission is in charge of reinforcing cooperation between the different national authorities and of promoting exchange of information and expertise by setting up a European product safety network between these national authorities.

When a national authority adopts a measure linked with a serious risk that may have an effect beyond its territory, it shall inform the European Commission via the system for the rapid

exchange of information between the Member States and the European Commission (also called the 'Rapex' system) of the identity of the product, the risks, the measures taken and the information on the distribution, including the destination countries. This information will be communicated to the other Member States. .

The European Commission can also approve rapid measures at Community level when it becomes aware of a serious risk in various Member States. After consulting the Member States

and a scientific committee when scientific questions arise, the Commission may adopt a decision (like the recall of the product, for instance) to be implemented by the Member States within less than 20 days.

9.1.2.1.2.Directive 2001/83 on medicinal products[79]

[79] Directive 2001/83 of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use, *O.J. L311,* of 28 November 2001, 67-128.

Directive 2001/83 on the Community code relating to medicinal products for human use imposes that no medicinal product may be placed on the market unless a marketing authorisation has been issued by the competent national authority.

9.1.2.1.2.1.Some key concepts[80]

In the Directive's framework a medicinal product is defined as any substance or combination of substances presented for treating or preventing disease in human beings or which may

[80] For a definition of all key concepts of the Directive and for a detailed analysis of the Directive's text see *Legally e-Health: Product Liability and Consumer Protection,* opcit.

be administered to human beings with a view to making a medical diagnosis or to restoring, correcting or modifying physiological functions.

On the other hand, a medicinal prescription is any medicinal prescription issued by a qualified professional person.

9.1.2.1.2.2.Directive's scope

Directive 2001/83 applies to industrially produced medicinal products for human use and intended to be placed on the market in the Member States.

9.1.2.1.2.3.Principle of authorisation

In the frame of the Directive, no medicinal product may be placed on the market, distributed, manufactured of imported unless a marketing authorisation has been issued by the competent national authorities of the relevant Member States. A

marketing authorisation may only be granted to an applicant established in the Community.

Before issuing an authorisation, the competent authority will check if the outer packaging, the immediate packaging and the package leaflet contain the necessary information (such as the name of the product, route of administration, adverse reactions, expiry date, etc.).

An authorisation holder may submit a request for recognition of this authorisation to other Member States.

However, even if medicinal products may not be put on the market of the EU Member States without a marketing authorisation to be delivered, some of these products might cause damages to patients' health.

Under certain conditions, the patient can obtain the repair of the undergone damage.[81]

9.1.2.2.Repairing a damage

When a defective product causes damages, rules contained in Council Directive 85/374 concerning liability for defective products will apply.[82]

This Directive aims at ensuring a high level of consumer protection against damage caused to health or property by a defective product. It also aims to reduce the disparities between national liability laws which distort competition and restrict the free movement of goods. Finally, it implements a system that extends the producer's liability (called the 'strict liability') in order to protect consumers.

Indeed, Directive 85/374 establishes the principle of objective liability or liability without fault of the producer, importer and under some conditions the supplier, in case of damage caused by a defective product. The producer, importer or supplier, will be liable and must pay compensation for damages caused to persons or properties but only for that resulting from a defect. The burden of proof on the injured person is lighter. The person does not have to prove that the producer was at fault or negligent; he just needs to prove the damage, the defect and the causal relationship between defect and damage.

When the producer, importer or supplier, is considered as liable, he must pay compensation for the damage caused to the person or to his properties, but only for that resulting from a defect.

[81] For more details about the advertising of medicinal products, see *Legally e-Health: Product Liability and Consumer Protection*, opcit.

[82] Council Directive 85/374 of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *O.J. L210,* of 7 August 1985, 29-33.

Though, in order to strike a reasonable balance between the interest of the consumer and the need to encourage innovation and technological development, the Directive contains some rules protecting the producer. Indeed, under some particular circumstances, the producer may be exonerated from all liability. Moreover, the injured person has a limitation period of three years to seek compensation. This period starts from the day on which the plaintiff became aware, or should reasonably have become aware of the damage, the defect and the identity

of the producer. After that, no further compensation will be possible. In any case the producer's liability is limited to a period of ten years from the date on which the producer put the product into circulation. This time limit is intended to preserve a balance between consumers and producers' interests.

9.1.2.3.After sales services

One of the important goals of the healthgrid systems used in the healthcare sector will be to deliver medicinal products or medical devices to patients, conform to ePrescription for example. The patients can thus acquire products necessary for the preservation of their health by means of the system.

Therefore in the eHealth arena, when the product delivered does not conform to what was foreseen in the contract, one will often refer to the relevant national legislation based on Directive 1999/44 of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantee.[83]

According to this Directive, when consumer goods are sold under a contract, the seller must deliver goods in conformity with the sale contract. Moreover, when a commercial guarantee exists, the seller or the producer who proposed it will have to respect some rules and will be legally bound to it as well as to the associated advertising. The commercial guarantee will have to be made available in writing (or another durable medium, such as an e-mail) and will have to contain some information. Anyone selling an eHealth product would have to comply with these rules, and conversely a purchaser of an eHealth product would have redress under them.

[83] Directive 1999/44 of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantee, *O.J. L171,* of 7 July 1999, 12-16.

Directive 1999/44 also establishes the conditions under which the seller will be liable when the consumer goods delivered do not conform to the sale contract at the time the goods were delivered. In this frame, the seller would however be exonerated from any liability if the consumer knew or should have known about the lack of conformity of the products. The seller would equally be exonerated from his liability in other situations.

Though, if his liability is established, the seller must respect the rights of the consumer and therefore repair or replace the good, free of charge, or if repairing the good is not possible, provide for an appropriate reduction of the good's price or rescind the contract.

9.1.2.3.1.Some key concepts[84]

In the framework of Directive 1999/44, the definition of the consumer is the same as the one of Directive 1997/7 on the protection of consumers in respect of distance contracts.[85]

The consumer has thus to be seen as any natural person who, in the contracts covered by the Directive, is acting for purposes which are not related to his trade, business or profession.

On the other hand, consumer goods covered by the Directive are any tangible movable item (except goods sold by authority of law, water and gas where they are not put up for sale in a limited volume or set quantity, and electricity).

Moreover, the seller is any natural or legal person who, under a contract, sells consumer goods in the course of his trade, business or profession, when the producer is defined as the manufacturer of consumer goods, the importer of consumer

[84] For a definition of all key concepts of the Directive and for a detailed analysis of the Directive's text see *Legally e-Health: Product Liability and Consumer Protection,* opcit.

[85] Directive 1997/7 on the protection of consumers in respect of distance contracts, *O.J. L144,* of 4 June 1997, 19-27.

goods into the territory of the Community or any person purporting to be a producer by placing his name, trademark or other distinctive sign on the consumer goods.

Finally the guarantee foreseen by the Directive's text is any undertaking by a seller or a producer to the consumer, given without extra charge, to reimburse the price paid or to replace, repair or handle consumer goods in any way if they do not meet the specifications set out in the guarantee statement or in the relevant advertising.

This term covers only commercial guarantees, which may be voluntarily proposed by the sellers, and not the 'legal guaranties', which exist just by effect of the law. The commercial guarantee offers protection in addition to that due by law. The legal guarantee is described in this Directive as the 'principle of conformity with the contract'.

9.1.2.3.2.Principle of conformity with the contract

The seller has to deliver to consumers goods that are in conformity with the contract of sale.

Consumer goods are presumed to be in conformity with the contract if they:

(a) comply with the description given by the seller and possess the qualities of the goods which the seller has held out to the consumer as a sample or model;
(b) are fit for the purposes for which goods of the same type are normally used;
(c) are fit for any particular purpose for which the consumer requires them and which he or she made known to the seller at the time of conclusion of the contract and which the seller has accepted;
(d) show the quality and performance which are normal in goods of the same type and which the consumer

can reasonably expect, given the nature of the goods and taking into account any public statements on the specific characteristics of the goods made about them by the seller, the producer or his or her representative, particularly in advertising or on labelling.

9.1.2.3.3.Liability of the seller in case of lack of conformity

The principle exists that the seller shall be liable to the consumer for any lack of conformity that exists at the time the goods were delivered.

Any lack of conformity, which becomes apparent within six months of delivery of the goods shall be presumed to have existed at the time of delivery unless proved otherwise or if this presumption is incompatible with the nature of the goods or the nature of the lack of conformity.

Where the final seller is liable to the consumer because of a lack of conformity resulting from an act or omission by the producer, a previous seller in the same

chain of contracts or any other intermediary, the final seller shall be entitled to look for repair with the responsible person.

In order to benefit from the protection, the consumer must inform the seller of the lack of conformity within a period of 2 months from the date on which he or she detected such lack of conformity.

Moreover, the seller's liability is limited to a two-year period from the date of the delivery of goods.

9.1.2.4.Exemption of liability

The seller is not liable if, at the time the contract was concluded, the consumer was aware, or could not reasonably be unaware of, the lack of conformity, or if the lack of conformity has its origin in materials supplied by the consumer.

The seller shall not be bound by public statements, if he:

- shows that he was not, and could not reasonably have been, aware of the statement in question,
- shows that, by the time of conclusion of the contract, the statement had been corrected, or
- shows that the decision to buy the consumer goods could not have been influenced by the statement.

But healthgrid systems are not only about data and products.

Services might also be delivered through healthgrids such as virtual courses in real time for under-graduates, graduates, young professionals in the case of medical eLearning or such as second opinions, demonstrations, or medical assistance of tourists or expatriates for example.

Equally simulations and modelling for therapy planning and computer-assisted interventions and large multi-centre epidemiological studies are typical clinical services that might be delivered through healthgrids.

What is the responsibility of the professionals concerned in the supply of these services?

9.1.3.Part I: C: Liability as regards Services

As mentioned above, services available through healthgrid application are diverse.

They might be passive services, such as supplies of general medical information through networks or Internet workstations for end-users. They might also be active services like medical advices or specific decision supports to clinicians, or might involve the collection of biomedical data for remote monitoring by clinicians.

Such services might conceivably cause damages to those who depend on it. A citizen might for instance follow a bad advice and fall ill, be harmed or even die. A clinician might follow the recommended procedure after using a decision support tool and might consecutively harm his patient.

The huge problem is that there is currently no European harmonization of liability rules for the delivery of services.

Liability in case of problems in the supply of services through healthgrid systems shall thus be governed by ordinary rules of law applicable in the different EU Member States, which might not be satisfactory.

The question is then whether this is also the case for services part of healthgrid systems.

Indeed, in the Netherlands, approximately 800.000 Dutch people over the age of 18 have been victims of errors due to the inadequate transfer of medical information.[86] Equally, in Europe, more than one million patients suffer injuries each year as a result of broken health care processes and system failures.[87]

[86] For more information on this subject, see IAKOVIDIS, I., *eHealth & Patient safety, Myths, Visions and Realities*, eHealth Congress, Brussels 19 October 2006.

[87] IOM, 2000 ; Starfield, 2000.

What about the responsibility problematic in such circumstances (Part II)?

9.2. PART II: LIABILITY AS REGARDS THE SYSTEM'S COMPONENTS

As stated by several researchers at the healthgrid Conference 2006, hold in Valencia in June 2006, the emergence of grid technology opens new perspectives to enable interdisciplinary research at the crossroads of medical informatics, bioinformatics and system biology impacting healthcare.[88]

How does this technology achieve such results?

The secret of the healthgrid lies in its components, i.e. in the products and the services composing it. Indeed, as already mentioned in this document a healthgrid is an environment where data of medical interest can be stored, processed and made easily available to different actors of healthcare, physicians, healthcare centres and administrations, and of course citizens.

It is thus composed of products such as Electronic Health Records (hereafter 'EHR') containing patients' information, computers, networks, powerful computing resources for analytical tasks, hospitals' equipments, scientific instruments and even medical devices as for instance wearable or portable mobile ICT systems.

It is also composed of services such as processing of medical images, data storage, management, archiving and retrieval, as well as data mining, or as simulation and modelling for therapy planning.

[88] BRETON, V., BLANQUER, I, HERNANDEZ, V., LEGRE, Y. and SOLOMIDES, T., "Proposing a roadmap for healthgrids", in *Challenges and Opportunities of healthgrids,* HERNANDEZ, V. and others, Amsterdam, IOS Press, 2006, p. 319.

In case of failing of the healthgrid system, there will be thus two systems of liability, as the failing will be due to a product (A) or to a service (B).

9.2.1.Part II: A: Liability as regards Products

The concept of the products components of healthgrids is a difficult one, because in practice it includes a lot of different things. These products will be either

software packages or hardware devices with embedded software (radio frequency identification location trackers for locating people and objects or remotely controlled medical devices).

Legally, these products will be covered by a range of European legislation.[89] First, before being marketed they will have to respect the conditions of Directive 2001/95 on general product safety[90]. A specific regulation will apply to medical devices placed on the market (1).

On the other hand, their sale will be covered by standard contracts for sale of goods -thus if the product fails to arrive or arrives late the standard clauses in the contract will apply which will allow the purchaser to pay less or to return the concerned product. Similarly national legislation based on Directive 1999/44 of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantee will apply. [91]

Finally, liability Directives will ensure that the purchaser has redress if the goods are not fit for the purpose they were sold for, while other EC regulations such as the Directive 2002/95 on the restriction of the use of certain hazardous substances in electrical and electronic equipment[92] (also called the 'RoHS' Directive) will provide the purchaser with certainty about certain aspects of a product's quality (2).

9.2.1.1.Directive 1993/42 on medical devices

When a product that will be placed on the market is considered as a medical device, specific additional rules regarding the safety of those particular products apply.

The Council Directive 93/42 concerning medical devices[93] aims notably to safeguards patients' and users' health and safety by

[89] For details on this point, see Chapter I, point B, of this document.

[90] Directive 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety, *opcit*.

[91] Directive 1999/44 of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantee, *opcit*.

[92] Directive 2002/95 of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, *O.J. L37*, of 13 February 2003, 19-23.

[93] Council Directive 93/42 of 14 June 1993 concerning medical devices, *O.J. L169*, of 12 July 1993, 1-43.

harmonizing the conditions for placing medical devices on the market and putting them into service.

Among other conditions, medical devices must be designed and manufactured in such a way that their use do not compromise the safety and health of patients, users and other persons when properly installed, maintained and used in accordance with their intended purpose.

The manufacturer should meet some essential requirements and notably eliminate or reduce the risks as far as possible.

Moreover EU Member States are involved in the protection of the patients. Indeed when one of them remark notes that a medical device conform to the Directive's prescriptions compromises the health and/or safety of patients, users or, where applicable, other persons, it shall take all appropriate interim measures to withdraw it from the market, prohibit or restrict it being placed on the market or put into service.

An information system has also been put in place in order to allow the Member States and the Commission to be aware of the incidents caused by medical devices.

9.2.1.1.1.Some key concepts[94]

According to the Directive's text, a 'medical device' means *" […] any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:*

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,*

[94] For a definition of all key concepts of the Directive and for a full comment on the Directive's text see *Legally e-Health: Product Liability and Consumer Protection,* opcit.

- *investigation, replacement or modification of the anatomy or of a physiological process,*
- *control of conception,*

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means".

The accessories which are not medical devices as such, but which are specifically intended to be used together with a device to enable it to be used as wanted by the manufacturer, shall be treated as medical devices.

Furthermore, electronic equipments and software must be regarded as enclosed within the definition of medical device, when they are manufactured or promoted for medical purpose. Indeed, according to the Guidelines relating to medical devices Directives[95] available on the website of DG Enterprise,[96] software related to the functioning of medical devices are medical devices on their own if placed on the market separately from the related devices. When a piece of software assists in making the diagnosis (like image enhancing software created for diagnostic purposes), or if it is used a therapeutic tool, it must be considered as a medical device. This is not the case for software used for the administration of general patient data.

Finally when a product has multiple purposes (such as PCs, printers, screens, etc.) it should only be considered as a medical device if it has a specific medical purpose (as underlined here above).

[95] These guidelines aim at promoting a common approach by manufacturers and Notified Bodies involved in the conformity assessment procedures according to the relevant annexes of the Directives, and by the Competent Authorities charged with safeguarding Public Health. Nevertheless, they are not legally binding. However, due to the participation of the aforementioned interested parties and of experts from Competent Authorities, it is anticipated that they will be followed within the Member States and, therefore, ensure uniform application of relevant Directive provisions.

[96] For details and references see *http://ec.europa.eu/enterprise/medical_devices/meddev/index.htm*.

As what regards the manufacturer, he is defined as the natural or legal person with responsibility for the design, manufacture, packaging and labeling of a device before it is placed on the market under his own name, regardless of whether these operations are carried out by that person himself or on his behalf by a third party.

The manufacturer's obligations set out in the Directive, must also be filled by the natural or legal person who assembles, packages, processes, fully refurbishes and/or labels one or more ready-made products and/or assigns to them their intended purpose as a device. This subparagraph does not apply to the person who, while not being a manufacturer within the meaning of the first subparagraph, assembles or adapts devices already on the market to their intended purpose for an individual patient.

9.2.1.1.1.1.General safety requirement

In the Directive's frame, manufacturers are obliged to place on the market or to put into service only medical devices that do not compromise the safety and health of patients, users and, where applicable, other persons, when properly installed, maintained and used in accordance with their intended purpose.

The manufacturer must design and manufacture medical devices in such a way that some 'essential requirements' are met, such as to take into account the generally acknowledged state of the art and to eliminate or reduce risks as much as possible (like the risks linked to the toxicity of certain materials and their incompatibility with biological tissues and cells, or the risks of contamination for persons involved in the transport, storage and use of medical devices)

Devices that are in accordance with the national provisions transposing the existing European harmonised standards will

be presumed by EU Member States as compliant with the essential requirements laid downed by the Directive.

Devices other than those which are custom-made or intended for clinical investigation must bear a CE conformity mark when placed on the market.

Products composing healthgrid systems that are electrical or constitute electronic equipments must respect other prescriptions (2).

9.2.1.2.RoHS Directive

When the products manufactured are electrical or constitute electronic equipments, like IT or telecommunications equipments, they shall respect the provisions of the RoHS Directive relating to the restriction of the use of certain hazardous substances in electrical and electronic equipment.

This Directive imposes to manufacturers to avoid the use of lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls (PBB) or polybrominated diphenyl ethers (PBDE) in those equipments.

However, the Directive does not currently apply to medical devices even if the definition contained in the Directive's text could cover electronic equipments and software.

Besides, the possibility of applying the RoHS Directive to the manufacturers of hardware products is debated. A possible interpretation of the Directive would be that hardware sold to medical equipment manufacturers in order to run medical equipments, but which retain all functions of a computer, will have to respect its

prescriptions. Nevertheless computers or other compounds installed into medical equipments which do not act as separate tools, but only operate the medical device, are to be considered as medical devices and are not concerned by RoHS Directive.

We can thus notice, to conclude, that the European rules do not miss to determine the responsibilities in case of imperfection of a product part of a healthgrid. As we already, certain directives even allow to protect the patients and the users more efficiently by introducing rules on the market introduction of medical devices and

on the insertion interdiction of certain hazardous compounds in electrical and electronic equipments.

Finally, it should be noted that national, European and international bodies are developing standards which apply to eHealth products. In particular, a specific standard called the 'CEN standard' was developed for EHRs. Indeed a transfer of information between two hospitals will work only if the two hospitals HER systems have the same data model. Another example is the development of the 'DICOM

standards' for medical digital images. Though these standards are not legally binding, they try to promote a certain uniformity of products composing healthgrids, which might have a decreasing impact on damages caused to patients and end-users and on the liability issue.

The situation is not also simple as regards the services (Part II B).

9.2.2.Part II: B: Liability as regards Services

As mentioned above, services composing healthgrids are diverse.

As services supplied through healthgrids, services composing the systems might cause damages to those who depend on it. Nowadays, there is for instance a lack of data and knowledge management services. A citizen might thus be seriously harmed or even die, if the information transmitted to the general practitioner treating him is not accurate or false, or if it is not supplied on time.

In the same way that for the services supplied by the system, for those who compose it, there is not either a liability rules harmonisation.

In case of problems with the services composing the healthgrid systems liability shall thus be governed by ordinary rules of law applicable in the different EU Member States.

Nevertheless, when these services are purely technical and provided through Internet, the Internet intermediary who transmits or stores third party information may benefit from an exoneration of liability in case of problems.

This will though not often be the case, as the grid infrastructure has only very recently started to migrate to web services.

However, when Internet services are part of a healthgrid, Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market[97] (also called the 'Directive on electronic commerce') might apply.

9.2.2.1.Health related websites

From the moment a service is proposed by Internet at the individual request of a recipient of services normally provided for remuneration, it is considered as an information society service. Accordingly the information duties established by the Directive on electronic commerce are to be respected. In the case of a doctor or a pharmacist running a health related website, this means that they will have to inform the website users of their identity, address, VAT number, etc. This information duty aims to enable the recipient of the service (professional or not) to identify properly the service provider and to ensure transparency of his activities.

In essence the purpose of the information duty is to allow the ultimate users to know against whom they can seek recourse if they should need to do so.

This principle of transparency of website providers is also included within the Communication made by the European Commission on the Quality Criteria for Health related Websites.[98] This Communication aims to increase the reliability of health related websites and also include other quality criteria that health related websites must comply with, like transparency of the website purpose, respect of privacy, accessibility adapted to the target audience, etc. Those quality criteria may

[97] Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J. L178,* of 17 July 2000, 1-16.

[98] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of Regions, "eEurope 2002: Quality Criteria for Health related Websites", *COM/2002/0667 final.*

serve as reference in the development of quality initiatives for health related websites.

For instance, telehome care might be a good solution for patients suffering from minor diseases. Medical devices as Vital Sign Monitors could help to monitor them and permit to threat them when necessary. Patients could then stay home and introduce their health data on a website (even via browser, cell phone or PDA) were web-based personal health records would be stored. To be reliable this system would have to respect the quality criteria set by the European Commission as what regards for instance accessibility for the patients. Indeed putting a medical device in the hand of persons not familiar with it might pose problems or even be dangerous. To be effective the system presented would have to be easy to use by patients.

On the other hand, when a health related website includes commercial communications (i.e. any type of communications promoting goods, services or the image of a company), the Directive on electronic commerce imposes additional duties to services providers. It requires, amongst other things that the person on whose behalf the commercial communication is made, be clearly identifiable and that commercial communication be clearly identifiable as such as well. The purpose of this rule is to avoid any confusion between advertising and any other type of information.

However, the Directive does not replace other legal texts imposing particular rules or restrictions relative to advertisement concerning regulated professions such as doctors or dentists.

In this context, it should be noted that Directive 2001/83, mentioned above, explicitly prohibits direct to consumer advertising of prescription medication. This applies whether the advertisement is made on paper or electronically. However,

given that direct to consumer advertising of prescription medication is permitted in the USA, many European citizens find American advertising on the Internet and buy directly from the USA.

When the advertisements made on the eHealth website concern medicinal products, some particular rules apply, as Directive 2001/83 authorises the advertising of medicinal products only if some conditions are met (delivery of a marketing authorization, no marketing for medicines only available on medical prescription or which requires intervention of a healthcare practitioner). Moreover, the advertising must encourage the rational use of the medicinal product.

Besides, according to Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices (also called the 'Unfair Commercial Practices Directive'),[99] any commercial practices (including advertising) directly connected with the promotion, sale or supply of a product (including service) to consumers must be fair. This Directive explains when a practice should be considered as unfair. All practices breaching the professional diligence requirements that materially distort the behavior of the average consumer will be considered as unfair, and therefore banned.

For instance, it is forbidden to promote a medicine as 100% guarantee without any side effects when the trader reasonably knows that the tests made cannot totally exclude them.

Directive 2005/29/EC thus bans unfair commercial practices such as misleading practices, failing to provide the consumer with the information needed or with false information, and aggressive practices, like harassment, coercion or undue

[99] Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, *O.J. L149*, of 11 June 2005, 22-39.

influence. The directive provides a black list of prohibited practices. It lists the practices that will be considered as unfair in all circumstances, such as unsolicited supply or use of bait advertising (when the lowed-price product is not available).

9.2.2.2.Liability exemptions

As mentioned above, Directive 2000/31 furthermore implements special rules of exoneration of liability.

These rules may minimize the risks for technical partners of eHealth services providers, who act as 'intermediaries'. For instance, in principle, a company that provides to one of its clients (an ePharmacy, for instance) a server space for web site hosting, will not be liable for the illegal sale of medical products or for the damage caused by wrong information delivered to patients.

The Directive establishes a special exoneration system of liability for some categories of Internet intermediaries providing information society services called 'Mere Conduit' (1), 'Caching' (2) and 'Hosting' (3) under specific circumstances.

9.2.2.2.1.Mere Conduit

The "Mere Conduit" is an information society service consisting of:

- the transmission in a communication network of information provided by a recipient of the service or
- the provision of access to a communication network.

When providing such a "Mere Conduit" service, the service provider is not liable for the information transmitted.

Though to benefit from this exemption of liability, the provider has to comply with several cumulative conditions:

- the provider does not initiate the transmission;

- the provider does not select the receiver of the transmission; and
- the provider does not select or modify the information contained in the transmission.

The acts of transmission and of provision of access include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for a

period longer than what is reasonably needed for the transmission.

However, the liability exemption does not affect the possibility for a Court or an Administrative Authority from asking the service provider that he prevents infringements or that he terminates it when they arise.

9.2.2.2.2.Caching

The “Caching” is an information society service consisting of the transmission in a communication network of information provided by a recipient of the service.

When providing such “Caching” service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request.

To benefit from this liability exemption, the provider has to comply with several cumulative conditions:

- the provider does not modify the information;
- the provider complies with conditions on access to the information;
- the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

- the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

As for 'Mere Conduit' services, the liability exemption does not affect the possibility for a Court or an Administrative Authority from asking the service provider that he prevents infringements or that he terminates it when they arise.

9.2.2.2.3.Hosting

The "Hosting" service consists of the storage of information provided by a recipient of the service.

When providing such "Hosting" service, the service provider is not liable for the information stored at the request of a recipient of the service.

To benefit from this exemption, the provider has to comply with several cumulative conditions:

- the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not

aware of facts or circumstances from which the illegal activity or information is apparent; or

- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The service provider may not benefit from this exemption when the recipient of the service is acting under his authority or his control.

This liability exemption does not affect the possibility for a Court or an Administrative Authority from requiring the service provider to prevent an

infringement or to terminate it, when it occurs, nor does it affect the possibility of establishing procedures governing the removal or disabling of access to information.

For example the Internet service provider that gives server space for a company's or an individual's website will not be liable for the information stored, when he does not know about the illegality of the information or if he is aware of the illegality of the information stored and prevents access to it.

When the provider has a control on the information -for instance when he is acting as an editor- he cannot benefit from the exoneration system provided for in the Directive.

9.2.2.2.4.No general obligation to monitor information

Finally, it is important to underline that when providing the three information services described above, providers can not be obliged to monitor the information which they transmit or

store, nor to seek actively facts or circumstances indicating illegal activity.

On the contrary, they may be obliged to promptly inform the competent public authorities of alleged illegal activities undertaken or of information provided by recipients of their services or to communicate to the competent authorities, at their request, information enabling the identification of recipients of their services with whom they have storage agreements.

To determine the responsibility or the absence of responsibility for each of the actors of the network becomes easier, at least when the grid infrastructure is located on the Internet.

Criteria others than the use of Internet also allow to determine the responsibilities in case of damage caused by the healthgrid system.

9.3. PART III: OTHER CRITERIA AS REGARDS LIABILITY

When products and services destined to patients or to end-users of the healthgrid or designed to be part of the system are supplied in certain circumstances, the responsibility of eHealth actors can be easier to determine.

9.3.1.Part III: A: Contracts

Much eHealth business will necessarily involve the conclusion of contracts. These contracts contain the description of the parties' obligations and, often, special

clauses. When one of the parties does not respect his obligation, the contract will thus constitute a helpful tool to determine the liabilities.

Under these circumstances, general national contract law will apply, transposing where applicable European legislation. For instance, the conclusion of contracts could occur for the delivery of eHealth products (pharmaceutical products for an ePharmacy) and for the provision of eHealth services (such as medical information,

medical advices or diagnosis). The latter includes the online provision of medical cares.

The delivery of eHealth products and the provision of eHealth services could also result from contracts concluded by electronic means. When such possibility of online contracting is offered, Directive 1997/7 on distance contracts applies,[100] as well as some rules of the Directive on electronic commerce.

The Directive on distance contracts applies only to contracts concluded between professionals and consumers, while the Directive on electronic commerce applies

[100] Directive 97/7 on the protection of consumers in respect of distance contracts, *O.J. L144,* of 4 June 1997, 19-27.

to business-to-consumer transactions and to business-to-business transactions, excepted when the professional parties are allowed to agree otherwise.

The application of two directives have for consequence that healthcare professionals, scientist, researchers, services providers and other actors of the healthgrid will have a duty to provide consumers/patients/users with some information.

Indeed, the Directive relative to Distance Contracts imposes on the supplier a duty to provide the recipient with written information (or another durable medium such as an e-mail or online information) about his identity, the product or the service and its price, prior to the conclusion of the contract.

From his part, the Directive on electronic commerce provides for a list of information relative to the formation of contracts, such as information on the

different technical steps to follow in order to conclude the contract or on the technical means proposed to identify errors.

The electronic contract concluded and the obligations failing on each of the parties will help to determine each party's liability, when the contact is not respected or when one of the obligations has not been fulfilled.

9.3.2.Part III: B: Electronic Signatures in the Health Setting

Healthcare professionals treating patients through the use of a healthgrid may use electronic signatures in order to authenticate their identity, their profession, as well as the fact that they are registered with a professional body.

A particular example of the use of the electronic signature, will arise in the case of electronic prescriptions where it will be necessary to ensure that the signatory has

the title of doctor and probably also that he is registered with the social security body, which allows the reimbursement of the medical fees.

An electronic signature aims to allow the person receiving electronic data (like an e-mail, an ePrescription, etc.) to be able to identify the origin/author of the information/data (identification) as well as to verify that the information has not been altered during its communication (integrity).

Different kinds of electronic signatures exist, from the very simple ones (the insertion of a scanned hand-written signature within an electronic document), to the most sophisticated ones, such as the signatures based on public key cryptography. This last kind of signatures implies the intervention of a trusted third party (called the 'Certification Service Providers') who creates certificates in order to allow the recipient to check the identity of the sender and the integrity of the message.

Directive 1999/93 on electronic signature provides the conditions for the legal recognition of any electronic signatures. When the signature is based on a public key cryptography system (advanced electronic signature), it benefits a more favourable regime. But any kind of electronic signature may enjoy some legal effects.

The main principle of the Directive is the introduction of a legal equivalence between the hand-written signature and the advanced electronic signature based on

a qualified certificate that meets some requirements. When the conditions are met, the advanced electronic signature is considered as having the same effect as a hand-written signature. In case of problems with a prescription or with a diagnosis, it will be easy to determine the author of the mistake.

Moreover, the legal equivalence cannot be *a priori* denied for any electronic signature as such. The fact that a signature is in electronic form and does not meet the requirements that make it possible to affirm automatically its equivalence with

the hand-written signature, does not allow the judges to refuse it. The legal effectiveness and admissibility in legal proceedings of an electronic signature cannot be refused simply because it is in electronic form or because it does not enjoy the conditions of an advanced electronic signature. Therefore, the legal value of a non-advanced eSignature must be determined case by case and may not be rejected *a priori*.

For instance, if a doctor uses his scanned signature for an ePrescription and after, in the framework of a trial, it must be proofed that the prescription was coming from

him, the judge cannot *a priori* refuse to consider this type of signature but have to analyse, with possibly the help of experts, the evidence value of this signature. The advantage of the use of advanced electronic signature is that, in the context of a trial, this type of signature is directly considered as having the same evidence value as the hand-written signature.

9.4. CONCLUSION

We saw that to determine the responsibilities of each actor within the framework of the healthgrid systems is not easy, also as these systems differ from each other. It is

all the same very important to manage to make it most exactly possible in order to stop the witch hunting which mostly take place when damages are caused to a patient. Doctors, at the front line in case of medical damages caused to patients are not serial killers and are not always responsible for all damages caused by healthgrids.

Develop rules and processes which allow to determine the responsibilities of each actor in case of errors and to introduce more legal safety, will favor the confidence

of the patients, but also of all the users of the network in healthgrid systems, which will facilitate their wide implementation on the territory of the European Union.

10.ANNEX III: INTELLECTUAL PROPERTY ISSUES

The healthgrid vision relies on setting up of grid infrastructures for medical research, healthcare and the life sciences.

This implies the availability of data organised in databases.

This also implies the availability of grid services, most notably for data and knowledge management.[101]

A full functioning healthgrid will then be composed of a data grid, i.e. a distributed and optimised storage of large amounts

[101] These services must be deployed on infrastructures involving healthcare centres (e.g. hospitals), medical research laboratories and public health administrations. For details on this point see, SOLOMONIDES, T., *Structuring and supporting Healthgrids Activities and Research in Europe (SHARE): towards a European Healthgrid, step on,* e-Science 2006, Amsterdam, 4-7 December 2006.

of accessible information and of a computing grid which implies the utilisation of numerous computers, computer programmes and other electrical components. The final part of a full healthgrid would be a knowledge grid or in other words, the intelligent use of a data grid for knowledge creation. This knowledge grid has not yet been deployed.

As we repeatedly mentioned in this document, a healthgrid is thus mainly composed of computer and computer programs and encompasses databases.

With the implementation of healthgrids on the territory of the European Union, the protection of databases will assume an increased importance, given that most grid services will be provided via electronic databases accessible online or offline or accessible via European-wide networks. Databases should therefore be accorded an appropriate level of protection so as to create an attractive environment for investments while safeguarding user's interests (Part I).

On the other hand, the deployment of Healthgrids on the territory of the European Union will mean that grid services

such as data management services, and products such as computer programs will be provided.

However, once a product or a service has been provided, it becomes very difficult, without adequate protection to ensure that a literary or artistic work or other protected matter will not be copied, transformed or exploited without the knowledge or the right holders and contrary to their interests. This is even truer when products or services are provided on a network vastly deployed.

Moreover, as one knows the implementation of Healthgrids will require the development of new services. In this framework, the creative effort, which provides a basis for investment in these new services, will be worth undertaking only if works and other matter are adequately protected by copyright.

Finally owing to the very nature of grids, any wide variation in the level of protection of works and other matter may place obstacles in the way of their development. Indeed, grids are

intended to be deployed on a large scale on the territory of the European Union. Thus, given the difficulty of verifying the use made of a work, and the scope for displacement of business which this opens up, there is a need for more far-reaching harmonisation of the protection provided by copyright and related rights.

The objectives listed above were mainly realised by three directives on copyright and related rights (II). As mentioned

above, this legal framework was completed with the Directive on the legal protection of databases.

10.1. PART I: INTELLECTUAL PROPERTY RIGHTS AND DATABASES

As researchers Laura Vilches Armesto and Philippe Laurent write, lawyers usually address medical data from a privacy point of view. Nevertheless, they continue by saying:

"However intellectual property is increasingly put forward when discussing the control, the use or the transmission of medical data. Even if medical data relates to patients and is moreover protected by very strict data protection and secrecy rules, this information is nonetheless "created", sorted, structured, explained and, more generally, processed by professional practitioners and medical administrations. Given this processing of the data and drafting of files and reports concerning health condition of patients, one could indeed assume that these intellectual investments should be worth some legal protection".[102]

This is not the case only for medical data. Some adequate legal protection is required for molecular data, cellular data, tissue data and even population data.

The Directive on the legal protection of databases, which was adopted in February 1996, could apply to databases constituted of medical, genetic or even general data, as regards its definition of a database. The first part of this chapter will thus be dedicated to the presentation of that directive (A).

The second part of this chapter will then be dedicated to the conflicts existing between copyright and patients' rights (B).

[102] VILCHES ARMESTO, L and LAURENT, P. "Intellectual property on medical data chimaeras and actuality", *Acts of the 16th World Congress on Medical Law*, Toulouse, 7-11 August 2006, p. 747-754.

10.1.1. Part I: A: Directive 96/9 on the Legal Protection of Databases

The purpose of the European legislators, by adopting the Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases,[103] was above all of providing harmonised copyright protection to databases.

The Directive also sought to create a legal framework that would establish the ground rules for the protection of a wide variety of databases in the information age. It did so by giving a high level of copyright protection to "original" databases[104] and a new form of *"sui generis"* protection to those databases which were not "original" in the sense of the author's own intellectual creation (those databases are also called "non-original" databases). In other words the directive introduced a new specific *sui generis* right for the creators of databases, whether or not these have an intrinsically innovative nature.

10.1.1.1. Directive's scope

The Directive defines a database as *"a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".*[105]

It does thus apply to databases in any form,[106] but does not apply to the software used in the making or operation of the database or to the works and materials contained therein.[107]

Nor does it affect the legal provisions covering patents, marks, designs and models or unfair competition that can apply to the database or to its contents.

[103] Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases, *OJ. L77,* of 27 March 1996, 20-28.

[104] See infra for a definition of this concept.

[105] Directive 96/9 on the legal protection of databases, art. 1, 2.

[106] Directive 96/9 on the legal protection of databases, art. 1, 1.

[107] Directive 96/9 on the legal protection of databases, art. 1, 3.

10.1.1.2.Copyright protection

Copyright can be defined as a free and automatic protection that is granted without any formality on literary and artistic works, which include amongst others, any production in the scientific domain.[108] Copyright is thus only granted to works that are expressed in a certain form and are original.

Copyright thus only applies to the structure of databases, but not to their contents. The article 3, 2, of the Directive foresees it moreover very specifically.

The protection of the scheme of a database under copyright law as defined by the Agreement on TRIPS is thus accorded when the scheme constitutes, by virtue of the choice or arrangement of the material, an intellectual creation particular to its author. In other words, one can say that copyright protection is granted to 'original' database as they are to a certain extend the expression of their authors' personality.[109]

A database of electronic health records could then be capable of being copyrighted, given that the healthcare practitioner has completed the records in an elaborate and original way.

This could also be the case for genetic[110] or tissue databases. Copyright protection could apply to the database comprised of tissue samples once the tissue data were coordinated and arranged in an original structure that could for instance help researchers.

The creator or the author of the database enjoys a group of exclusive rights. He shall indeed have the exclusive right to carry out or to authorise:

---

[108] Definition proposed in "Intellectual property on medical data chimaeras and actuality", *opcit,* p. 747.

[109] On the contrary, a "non-original" database can be defined as a structure which does not, in its arrangement, reflect choices of the creator, but in which this mast one has made substantial investment.

[110] For a detailed analysis of copyright protection for genetic databases in the United States see, Ray K. HARRIS and Susan Stone ROSENFIELD, "Copyright Protection for Genetic Databases", *45 Jurimetrics,* 2005, p. 225-250.

(a) temporary or permanent reproduction by any means and in any form, in whole or in part;
(b) translation, adaptation, arrangement and any other alteration;
(c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community;
(d) any communication, display or performance to the public;
(e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).[111]

Though there are exceptions to this rule. Indeed, the legitimate user of a database may perform all the acts referred to in article 5 of the Directive that are necessary for using the database.

On the other hand, Member States have the option of providing for limitations on the rights set out in article 5 in some specific circumstances such as when the database is used for the purposes of public security or of an administrative or judicial procedure.[112]

However, the protection granted to databases by Directive 96/9 might seem insignificant with the efforts and the energy demonstrated by data grids creators in other to retrieve in each case, molecular, cellular, tissue or personal data. Only the structure of these databases is protected, while value for sure still resides in the samples of the databases for development of enhancements, competing technologies or follow-on products.

That is certainly the reason why in addition to the copyright arrangements, provision has also been made for *"sui generis"* protection.

[111] Directive 96/9 on the legal protection of databases, art. 5.
[112] For details on this point see Directive 96/9 on the legal protection of databases, art. 6.

10.1.1.3.Sui generis protection

The Directive 96/9 introduced another protection for databases beside copyright. It created a new exclusive *sui generis* right for database producers.

Sui generis rights protect the substantial investment of the database producer from a quantitative and qualitative perspective, in the obtaining, verification or presentation of the contents of the database.[113]

There is thus a different protection granted for any investment made (financial and in terms of human resources, effort and energy) in the obtaining, verification or presentation of the contents of a database.

So, in terms of protection granted, the difference between the structure, the content and the investment made for the development of a database is very important. Copyrights protect the structure of databases, while *sui generis* rights protect the investment made for the development of databases. The contents of these databases are sometimes protected as for them by intellectual property rights or by other types of legal protection.[114]

In the framework of the *sui generis* protection, the creator of a database (i.e. the person who made the investment), whether a natural or a legal person can prohibit the unauthorised retrieval and/or re-use of its contents.[115] Protection against unauthorised retrieval or re-use is accorded to databases whose maker is a

[113] Directive 96/9 on the legal protection of databases, art. 7, 1. See also recitals 40 to 42 of the Directive.

[114] On this point, see point B infra.

[115] Directive 96/9 on the legal protection of databases, art. 7, 1. The terms extraction and re-utilisation are defined in article 7, 2 of the Directive. In this framework, extraction shall be seen as the permanent or temporary transfer of all or of a substantial part of the contents of a database to another medium by any means or in any other form. On the other hand, re-utilisation shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community.

national, a company or an undertaking resident in or having his/its registered office, central administration or principal place of business in the Community.

On the contrary and as underlined by researchers Laura Vilches Armesto and Philippe Laurent *"non-substantial extractions and reuses may be undertaken by third parties, without the right owner's authorisation, as long as these acts are not made in a repeated and systematic way that would imply a conflict with the normal exploitation of the database or produce an unreasonable prejudice to the legitimate interests of the database's maker".*[116]

The fact that non-substantial parts of a database may be extracted from it and re-used in another database might cause a prejudice to other interests than the ones of the database creator.

For instance, the extraction of information from a database containing medical records might cause a prejudice to patients' rights. There can thus be a contradiction between this right to re-use non-substantial parts of a database to create another database for example and the legislation applicable to the protection of the data which requires for any re-use of data relative to a patient, the agreement of this one.

Furthermore, on this topic it is important to underline that *sui generis* rights form pecuniary rights and as such can be transferred, assigned or granted under contractual licence.[117]

This principle applies irrespective of the eligibility of the database for protection by copyright or by other rights. Moreover, it applies irrespective of eligibility of the contents of that database for protection by copyright or by other rights such as patient's rights.[118]

[116] Directive 96/9 on the legal protection of databases, art. 7, 5, a contrario.
[117] Directive 96/9 on the legal protection of databases, art. 7, 3.
[118] Directive 96/9 on the legal protection of databases, art. 7, 4.

Finally, it is also important to mention that the right to prevent the unauthorised retrieval of the contents of a database extends for a period of 15 years with effect from the date on which the creation of the database was terminated.[119]

The combination of these two principles, i.e. *sui generis* rights form pecuniary right and *sui generis* protection lasts for a period of 15 years, may constitute an impediment for the deployment of Healthgrids.

Database creators could for example charge third parties wanting to develop data grids before granting them their *sui generis* rights under contractual licence. They might thus be an impediment in terms of costs to the implementation of Healthgrids. On the other hand, in the pharmaceutical sector, researchers might claim *sui generis* rights on certain databases. Such claims could delay the release of other products that could have been discovered on the basis of the information contained in the first database compiled in another way.

By introducing the *sui generis* protection, the purpose of the European Commission was to induce an increase in the European database industry's rate of growth and in database production. The Commission (DG Internal Market and Services) published on 12 December 2005, the first evaluation of its directive. This evaluation also looks at whether the scope of the right targets those areas where Europe needs to encourage innovation.

The evaluation was conducted on the basis of a 2005 online survey addressed to the European database industry and of the

[119] Directive 96/9 on the legal protection of databases, art. 10, 1. In the case of a database which is made available to the public in whatever manner before expiry of the period provided for in paragraph 1 of article 10,the term of protection by that right shall expire fifteen years from the first January of the year following the date when the database was first made available to the public (art. 10, 3). Finally any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection (art. 10, 3).

Gale Directory of Databases (the "GDD"), which is the largest existing database directory.

Indeed, the vague terms used in the Directive to define the *sui generis* right seem to have caused considerable legal uncertainty. Also the scope of the *sui generis* right was severely curtailed in a series of judgments rendered by the European Court of Justice in November 2004.[120]

On publication, DG Internal Market and Services invited stakeholders to comment on four options: repeal the whole directive (option 1); withdraw the *sui generis* right while leaving protection for creative databases unchanged (option 2); amend the *sui generis* provisions in order to clarify their scope (option 3); maintain the status quo (option 4).[121]

In that context, Internal Market and Services Commissioner Charlie Mc Creevy said:

"Databases are a key part of Europe's economy in the information age. I want to make sure that EU rules encourage database production, not hinder it. This evaluation puts us on the right track. I now call on the industry and other stakeholders to comment and tell us more about how EU database rules affect them".

The open consultation will be concluded with a final assessment by the Commission on whether legislative changes are needed or not.

Whatever is the decision of the Commission, it will change nothing to the contradiction which can exist between copyrights and patients' rights (B).

[120] The ECJ's differentiation between the resources used in the creation of the contents of a database and the obtaining of such data in order to assemble a database demonstrate that the new right comes precariously close to protecting basic information.

[121] Public consultation was initially open until 12 March 2006, but extended to 31 March 2006. 55 contributions were received.

10.1.2.Part I: B: Copyrights and Patients' Rights

As evoked earlier in point A of this Chapter, copyrights can oppose patient's rights.

Indeed, a database author has the right to control the reproduction and the communication of his work to the public. But in the case of databases constituted of electronic health records, cellular or tissues, the work is *"[…] created with data relating to patient(s), (their) bodies, (their) health and the treatment they undergo. These data (are) subject to very strict sensitive data protection and privacy rules".*[122]

Some authors and researchers think that the patient's rights and the protection of sensitive data have to dominate on copyright. This would have a direct impact on the exercise of authors' exclusive rights. For instance, an author could not anymore exercise his exclusive rights alone.

If it is desirable that copyrights on databases composed of medical data, genetic data and other materials relating to patients, should never distorts patients' rights, taking the path described above could impede the development of databases and as a consequence the development of Healthgrids.

Indeed, if there were only rare cases where an author can claim copyrights on his work, nobody would be willing to make the investment necessary for the creation of a database.

One of the possible solutions would be to introduce a distinction between various types of data, as the medical data and the data of health or sanitary data.

In the case of electronic health records, it would be advisable among others to determine the status of the personal notes of the doctor. Indeed most of the blockings seem to come from the

[122] "Intellectual property on medical data chimaeras and actuality", *opcit,* p. 748.

absence of clear and precise definition of the notion of medical datum.[123]

Finally, it is important to underline that if copyrights are a sort of reward (at least a financial one) for the creators of databases, they also constitute a brake in the development of Healthgrids (II).

10.2.PART II: INTELLECTUAL PROPERTY RIGHTS AND GRIDS' COMPONENTS

On 27 July 1995, the European Commission issued a green paper on copyright and related rights in the information society.[124] The purpose of this green paper was to set out the background to a number of questions of copyright and related rights as the information society was developing.

In his first part, the paper thus described how the information society was ought to function and highlighted the issues that arise as a result of the emergence of that society. The second part of the paper picked out nine points regarding copyright and related rights that the Commission believes should be given priority in order to ensure that the information society could function properly.

Indeed, in that time, the Commission believed that copyright and related rights could provide an incentive for the creation of and investment in new works and other protected matter and their exploitation, thereby would contribute to improved competitiveness, employment and innovation. Latter, this proved to be true.

But in that time, even if the information society could start developing on the basis of Directive 91/250 on the legal protection of computer programs (A), the legal framework of

[123] Philippe VANLANGENDONCK, « Le dossier médical électronique : problèmes de vie privée et de responsabilité », sur *http://www.droit-technologie.org*, p. 1-10. For developments on this topic see the Roadmap document.

[124] COM(95)382, not published in the Official Journal.

the European Union was not yet ready for the deployment of vast networks. Indeed, owing to the very nature of such networks, any wide variation in the level of protection of works and other protected matter may place obstacles in the way of their development.

A Community-wide harmonisation of the national legislations available for the protection of copyright and certain related rights mainly took place in the shape of two directives (B and C). This legal framework was completed with the Directive on the legal protection of databases mentioned above.

With all theses measures, the Community seemed to have provided a proper legal framework for the development of services in the information society.

What about the development of Healthgrids on a European-wide basis?

It seems that the legal framework developed within the European Union allows a harmonised protection of copyright and related rights in all the EU Member States. In this sense, the harmonisation of the national legislation will favour the implementation of Healthgrids as services can circulated freely without any barriers and that market will not be fragmented.

On the other hand, copyrights can constitute an impediment in the implementation of Healthgrids, given that copyright law treats computer software as a copyrightable literary work, the same as a play or a novel. The copyright owner has the exclusive rights to reproduce his work, prepare derivative works, distribute copies to the public, perform the work publicly and display the work publicly. Under these circumstances any natural or legal person would have to pay to use computer programs while they constitute one of the most important compound of Healthgrids.

The open source software approach could then be a solution to help the development and implementation of Healthgrids. In the

United States, the open source model actually uses copyright and contract principles to retain control of the work and could thus encourage use without dedicating the work to the public domain.[125]

But for the moment let us analyse at first the legal framework in which the systems elaborate.

10.2.1. Part II: A: Directive 91/250 on the legal protection of computer programmes[126]

The Directive on the legal protection of computer programs was a real European 'first' for copyright law, the first copyright measure to be adopted following the publication of the White Paper on completing the Single Market by 1992.

The objective of the Directive was to harmonise Member States' legislation regarding the protection of computer programmes in order to create a legal environment that will afford a degree of security against unauthorised reproduction of such programmes.

10.2.1.1. Protection's subject matter

In accordance with the Directive's provisions, the Member States are obliged to protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works.[127]

The ideas and principles that underlie any element of a computer program, including those that underlie its interfaces, are not protected by copyright.[128]

---

[125] See Dennis M. KENNEDY, "A primer on open source licensing legal issues: copyright, copyleft and copyfuture, *20 ST. LOUIS U. PUB. L. REV.,* 2001, 345, p. 359-360; David MCGOWAN, "Legal implications of open-source software", *U. ILL. L. REV.,* 2001, 241, p.242-243. More generally see Open Source Initiative, at http://www.opensource.org.

[126] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *O.J. L 122*, of 17 May 1991, 42–46.

[127] Directive 91/250 on the legal protection of computer programs, art. 1, 1.

[128] Directive 91/250 on the legal protection of computer programs, art. 1, 2.

A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.[129]

10.2.1.2.Authorship of a computer programme

In general, the author of a computer program is the natural or legal person or group of natural persons who created it.

Where collective works are recognised by the legislation of a Member State, the person considered by the legislation of that Member State to have created the work is deemed to be its author.[130]

In the case of a program created by a group of natural persons, the exclusive rights are owned jointly.[131]

Finally, the Directive also provided for the situation of copyright ownership of work for hire. Indeed, where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer alone will be entitled to exercise all economic rights in the program, unless otherwise provided for by contract.[132]

Protection is accorded on the basis of residence, nationality and first publication as laid down by the relevant Member State.

10.2.1.3.Copyright protection

Subject to the provisions of Articles 5 and 6 of the Directive, the exclusive rights of the author of a computer program include the right to perform or to authorise:

[129] Directive 91/250 on the legal protection of computer programs, art. 1, 3.
[130] Directive 91/250 on the legal protection of computer programs, art. 2, 1.
[131] Directive 91/250 on the legal protection of computer programs, art. 2, 2.
[132] Directive 91/250 on the legal protection of computer programs, art. 2, 3.

(a) the permanent or temporary reproduction of his computer program by any means and in any form, in part or in whole;[133]
(b) the translation, adaptation, arrangement and other alteration of his computer program and the reproduction of the results thereof without prejudice to the rights of the persons who alters the program;
(c) the distribution, including the rental, of his original computer program or of copies thereof.[134]

10.2.1.4.*Exceptions to the protection granted*

The Directive provides for certain exceptions regarding copyright, mainly in the situations described below.

The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract insofar as it is necessary for that use.[135]

Equally, a person having a right to use a copy of a computer program is entitled to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to perform.[136]

There is also provision for a derogation that would allow the decompilation[137] of a program under certain limited conditions

[133] Insofar as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the author of the program.

[134] On this point, it is important to underline, what the Directive also does, that the first sale in the Community of a copy of a computer program by the right holder or with his consent exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental or the program or copy thereof.

[135] Directive 91/250 on the legal protection of computer programs, art. 5, 2.

[136] Directive 91/250 on the legal protection of computer programs, art. 5, 3.

[137] Decompilation can be defined as reproducing the code source of the computer program and translating its form in order to obtain the information necessary to achieve the interoperability of an independently created program with other programs.

and with the aim of achieving the interoperability of an independently created computer program.[138]

10.2.1.5.Special protection measures

Special protection measures will be taken against a person committing any of the acts listed hereunder:

(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is a pirated copy;
(b) any possession for commercial purposes of a copy of a computer program knowing, or having reason to believe, that it is a pirated copy;
(c) any act of putting into circulation or the possession for commercial purposes of any means with the intended purpose of facilitating the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

These special protection measures shall be provide for by the Member States, each one in accordance with its national legislation, by virtue of Article 7, 1, of the Directive.

10.2.1.6.Terms of protection

Protection shall be granted for the life of the author and for fifty years after his death or after the death of the last surviving author.

On the other hand, the term of protection is fifty years from the time the computer program is first made available to the public when the computer program is an anonymous work, when it was made available to the public under a pseudonym or when a legal person is designated as the author.

[138] For more details on this point, see Directive 91/250 on the legal protection of computer programs, art. 6.

The Directive 93/98 on harmonising the term of protection of copyright and certain related rights, mentioned below, extended the duration of copyright protection to seventy years.

10.2.1.7.Directive's evaluation

On 10 April 2000, the European Commission addressed a report to the Council, the European Parliament and the Economic and Social Committee on the implementation and effects of the Directive.[139]

This report contained an evaluation of the Directive's implementation in the Member States. It showed that the Directive's objectives had been achieved and that its effect on the software sector had been satisfying. The Directive had indeed improved the situation of the computer program sector in four ways: piracy was reduced, employment increased, a

[139] COM(2000)199 final.

switch had been operated to open systems together with a harmonisation as to computer programs created by employees.

However, the Commission stated that she might have to examine certain imperfections in greater depth. In particular, some specific problems had been raised as regards the distribution right and communication to the public, back-up copies, remedies and the technical provisions (i.e. the same problems that one will be confronted with for Healthgrids' implementation).

10.2.2. Part II: B: Directive 93/98 on harmonising the terms of protection of copyright and certain related rights

As mentioned above, Directive (93/98/EEC)[140] harmonised the terms of protection of copyright and neighbouring rights. The Directive establishes a total harmonisation of the period of protection for each type of work and each related right in the Member States -e.g. 70 years after the death of the author for works and 50 years after the event setting the time running for neighbouring rights. Furthermore, it dealt with other issues, such as the protection of previously unpublished works, of critical and scientific publications and of photographic works.

The Directive sets the duration of copyright in a literary or artistic work at 70 years after:

(a) the death of the author of the work[141] or
(b) the date on which the work was lawfully made available to the public, in the case of an anonymous or pseudonymous work.[142]

It sets the term of protection for cinematographic or audiovisual works at 70 years after the death of the last of the following persons to survive, i.e. the principal director, the author of the

[140] Council Directive 93/98/EEC of 29 October 1993 on harmonising the term of protection of copyright and certain related rights, *O.J. L290*, of 24 November 1993, 9-13.
[141] Directive 93/98/EEC, art. 1, 1.
[142] Directive 93/98/EEC, art. 1, 3.

screenplay, the author of the dialogue and the composer of music specifically created for use in the cinematographic or audiovisual work.

On the other hand, it sets the term of protection for related rights at 50 years.

The terms laid down in the Directive are calculated according to the circumstances, from the date of the performance, the date of the publication or communication of the fixation, or the date of the broadcast.

But the interesting point is that the term of protection starts to run at the same time in every Member State. It is calculated from the first day of January of the year following the event which gives rise to it.[143] In this framework, when the work is originated in a third country or when the author is not a Community national, the protection granted by the Member States expires on the same date as the protection granted in the country of origin of the work, but must never exceed the term laid down in the Community.

Finally, the Directive provides that the Member States are required to notify the Commission immediately of any plan to grant new related rights. They are also required to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive.

An enormous work of harmonisation of the national legislation on the protection of copyright and related rights was thus achieved through Directive 93/98. The work continued in the direction of an adaptation of the member States national legislation performed by Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society.

[143] Directive 93/98/EEC, art. 8.

10.2.3. Part II: C: Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society[144]

This Directive aimed to adapt legislation on copyright and related rights to technological developments and particularly to the information society. The objective was to transpose at Community level the main international obligations deriving from two Treaties[145] concerning copyright and related rights, adopted in December 1996 in the framework of the World Intellectual Property Organisation (also named 'WIPO').

10.2.3.1. Directive's scope

Unless otherwise provided, the Directive applies without prejudice to existing provisions relating to the legal protection of computer programs, rental and lending rights and certain rights related to copyright in the field of intellectual property, copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission, the term of protection of copyright and certain related rights and the legal protection of databases.[146]

The aim of the Directive was also to deal with three main issues, i.e. reproduction rights, the right of communication and distribution rights.

Indeed, as regards the first issue, the Directive should define the scope of the acts covered by the reproduction right with regard to the different beneficiaries. This should be done in conformity with the *acquis communautaire*. A broad definition of these acts was indeed needed to ensure legal certainty within the internal market.[147]

---

[144] European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *O.J. L 167*, of 22 June 2001, 10-19.

[145] These two Treaties were the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

[146] Directive 2001/29/EC, recital 20.

[147] Directive 2001/29/EC, recital 21.

The Directive thus concerns the legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society.[148] Moral rights remain outside the scope of the Directive.[149]

10.2.3.2.Reproduction rights

Under Article 2 of the Directive, Member States are to provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:

(a) for authors, of the original and copies of their works;
(b) for performers, of fixations of their performances;
(c) for phonogram producers, of their phonograms;
(d) for the producers of the first fixation of films, in respect of the original and copies of their films;
(e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.

10.2.3.3.Right of communication

Moreover, by virtue of Article 3, 1 of the Directive, Member States are to provide authors with the exclusive right to authorise or prohibit any communication to the public of the originals and copies of their works, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

The same applies as regards the making available to the public of protected works in such a way that members of the public may access them from a place and at a time individually chosen by them:

(a) for performers, of fixations of their performances,
(b) for phonogram producers, of their phonograms,

[148] Directive 2001/29/EC, art. 1.1.
[149] Directive 2001/29/EC, recital 19.

(c) for the producers of the first fixation of films, in respect of the original and copies of their films,
(d) for broadcasting organisations, of fixations of their broadcasts - regardless of the method of transmission.

10.2.3.4.Distribution rights

Finally, the Directive harmonised for authors the exclusive right of distribution to the public of their works or copies thereof. This distribution right is exhausted where the first sale or other transfer of ownership in the Community of a copy is made by the right holder or with his consent.[150]

10.2.3.5.Exemptions and limitations

The Directive also laid down a number of exceptions to the right of reproduction and the right of communication in his Article 5.

There was to begin with, a mandatory exception to the right of reproduction. This exception was introduced in respect of certain temporary acts of reproduction which are integral to a technological process, the purpose of which was to enable the lawful use or transmission in a network between third parties by an intermediary of a work or other subject-matter and which has no separate economic significance.

The Directive also contained a provision for other non-mandatory exceptions to the rights of reproduction or communication. In these cases, they are accorded at national level by the Member State concerned.

10.2.3.6.Rights of reproduction and communication

In the Directive's framework, the exemptions and limitations relating to the rights of reproduction and communication are optional and particularly concern the "public" domain.

[150] Directive 2001/29/EC, art. 4.

For three of these exceptions -reprography, private use and broadcasts made by social institutions- the right holders are to receive fair compensation.
With regard to the exceptions or limitations to distribution rights, these are accorded depending on the exceptions relating to reproduction or communication.

10.2.3.7.Protection of technological measures[151]

The Member States were equally obliged to provide legal protection against the circumvention of any effective technological measures[152] covering works or any other subject matter. This legal protection also related and still does to "preparatory acts" such as the manufacture, import, distribution, sale or provision of services for works with limited uses.

Nevertheless, for some exceptions and limitations, in the absence of voluntary measures taken by right holders, the Member States had to ensure the implementation of an exception or limitation for those who may benefit from it. The Member States had also the choice to take such measures with regard to the exception for private use, unless right holders, in accordance with the economic damage test, had already made reproduction for private use possible.

[151] Directive 2001/29/EC, art. 6.

[152] For the purposes of the Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the right holder of any copyright or any related to copyright as provided for by law or sui generis right provided for in Chapter II of Directive 96/9/EC.

10.2.3.8.Protection of rights-management information[153]

Finally Member States had to provide for adequate legal protection against any person knowingly performing, without authority, any of the following acts:

(a) the removal or alteration of any electronic rights-management information;

(b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected from which electronic rights-management information has been removed or altered without authority.

[153] Directive 2001/29/EC, art. 7. For the purposes of the Directive, the expression "right-management information" means any information provided by the right holders which identifies the work and other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other right holder, or information abut the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.