

**SIXTH FRAMEWORK PROGRAMME
PRIORITY 2
Information Society Technologies**



026990

Ethical Manual HUMABIO

Deliverable No. (use the number indicated on technical annex)		D1.1	
Workpackage No.	WP1	Workpackage Title	Use cases, legal and ethical requirements
Task No.	T1.3	Task Title	Legal & ethical issues and project policy
Authors (per company, if more than one company provide it together)		Dr. Alex Bullinger (COAT) Marcel Delahaye (COAT)	
Status (F: final; D: draft; RD: revised draft):		D	
File Name:		HUMABIO Ethical Manual	
Project start date and duration		01 January 2006, 30 Months	

List of abbreviations

Abbreviation	Definition
BAN	Body Area Network
ISP	Internet Service provider
ITT	Invitation to tender
LAN	Local Area Network
LREC	Local Research Ethics Committee
PDPU	Personal Data Processing Units
SAP	Secure Authentication Protocol
SSL	Secure Socket Layer
SET	Secure Electronic Transactions
VPN	Virtual Private Network
WAN	Wide Area Network

Table of contents

LIST OF ABBREVIATIONS	2
TABLE OF CONTENTS	3
EXECUTIVE SUMMARY	7
1 INTRODUCTION	8
1.1 PROJECT DESCRIPTION	8
1.1.1 EU ETHICAL GUIDELINES.....	10
1.1.2 LEGISLATION OF THE EUROPEAN COMMISSION	10
1.1.3 INTERNATIONAL CONVENTIONS AND DECLARATIONS	11
1.2 PILOT SETUP	12
2.1 PARTICIPANT GROUPS AND THEIR CONSENT.....	23
2.2 BASIC ELEMENTS OF INFORMED CONSENT	24
2.3 GUIDELINES FOR COMPILING THE INFORMED CONSENT FORM.....	25
2.4 INFORMED CONSENT AND THOSE UNABLE TO READ THE FORM	27
2.5 THE LEGAL POSITIONS	27
3 SECURITY ISSUES IN HUMABIO	29
3.2 THE SECURITY ISSUE.....	31
3.3 MEASURES FOR IMPROVING THE SECURITY IN HUMABIO.....	32
3.3.1 <i>Develop Information Security Policies and Standards</i>	33
3.3.2 <i>Design the Information Security Architecture and Processes</i>	33
4 PRIVACY (AND TRANSPARENCY) ISSUES IN HUMABIO	36
4.1 GENERAL PRINCIPLES	38
4.1.1 OVERVIEW ABOUT DIFFERENT CONFIDENTIALITY PRINCIPLES	38
4.2 ANONYMISATION AND CODING	40
4.3 INTERNATIONAL AND EUROPEAN INSTRUMENTS IN THE FIELD OF DATA PROTECTION.....	41
4.4 TECHNICAL IMPLEMENTATION IN HUMABIO	49
4.5 HUMABIO PRIVACY POLICY	49
5 HUMABIO IDENTITY MANAGEMENT	51
6 RISK ASSESSMENT	51
6.1 “CONFLICT OF INTEREST”	52
7 THERAPEUTIC AND NON-THERAPEUTIC RESEARCH	53
8 DECEPTION AND DEBRIEFING	54
8.1 DECEPTION.....	54
8.2 DEBRIEFING.....	54
9 ORGANIZATION AND INSURANCE ISSUES	55
9.1 ETHICS CONTROL COMMITTEE	55
9.2 ACCESSIBILITY OF FACILITIES AND SERVICES	55
9.3 REIMBURSEMENT SCHEMES.....	55
9.3.1 <i>Incentives for participants</i>	55
9.3.2 <i>Legal basis for reimbursements as incentives</i>	56

9.3.3 <i>The amount to pay</i>	56
9.3.4 <i>Type of payment</i>	57
10 FUTURE STEPS	58
11 HUMABIO ETHICS ADVISORY BOARD	59
12 RECOMMENDATIONS	60
13 REFERENCES	61
ANNEX I TEMPLATE ON ETHICAL & LEGAL ISSUES	63
ANNEX II HUMABIO INFORMED CONSENT FORM TEMPLATE	71

List of Figures

Figure 1: HUMABIO Biometric Authentication Core for the pilots	14
Figure 2:: HUMABIO concept for vehicle application.....	17

List of Tables

Table 1: HUMABIO Application.....	13
Table 2: Ethical issues in the truck pilot	16
Table 3: Ethical issues in the office application.....	18
Table 4: Ethical Issues for restricted area pilot.....	20
Table 5: General Objectives of HUMABIO	21
Table 6: National and International approaches about confidentiality principles.....	40

Preface

With regard to the **DoW WP 9** this Deliverable describes the potential **ethical aspects** of HUMABIO regarding its objectives, the methodology and the possible implications of the results. The Ethics considered are for the development of the project, and not for the eventual use of the system.

“We assure that within HUMABIO we will fully respect and promote the ethical principles that are guiding our research activity: We conform to the rights / ethical principles of human dignity, integrity of the person, democracy, prohibition of degrading treatment, cultural, religious and linguistic diversity, equality, freedom of expression and information, the freedom of research, consumer protection, the right of the child, the elderly and the handicapped, non discrimination, privacy, protection of personal genetic data, as they are described in the Charter of European Fundamental Rights. Our research is only performed for purposes of betterment of the lives of European citizens.”

“All national legal and ethical requirements of the Member States where the research is performed will be fulfilled. All laboratory based experiments, feasibility studies and pilots - before conducted within HUMABIO – need the unconditioned approval of the respective responsible local ethics committees, to make sure that the national legal and ethical requirements of the country where the research is performed will be followed.”

“Every experiment undertaken within HUMABIO will be verified by the local ethics committee and the Ethics Advisory board. In doing this, interests of the donors will be safeguarded.”

In accordance with these commitments written in the DoW (p.93) the mentioned ethical principles will be specified in this Deliverable. Special emphasis will be given to the ethical evaluation of the planned pilots.

Executive Summary

This Ethics Manual defines the ethics code of conduct of research within HUMABIO. Key ethical and legal issues have been identified (see pilot plan). A relevant project policy towards examining these issues has been developed. Furthermore, it has been specified which data are essential for the project and which should be excluded from retention. All project partners' deliverables and pilots conduct will be scanned on behalf of the information listed in this manual. Relevant national and international European conventions (i.e. Helsinki Declaration) are fully integrated in the manual. Utilising T1.3 Template on "ethical and legal issues", specific national standards and local conventions of ethics committees are being scanned and integrated in the Manual. All in all the Manual is conceptualised to offer guidelines for all research performed within the auspices of HUMABIO.

After a project description where HUMABIO is introduced and relevant ethical concerns regarding the pilot tests are proposed (**Chapter 1**), detailed information about informed consent, such as basic elements of and guidelines for compiling informed consent, is provided (**Chapter 2**). Detailed guidelines on security issues will be described in **Chapter 3**. **Chapter 4** (Privacy of individual data), is dedicated to the confidential use of personal data. The issue on how confidentiality of personal data can be maintained and guaranteed leads to different methods of anonymisation, that are listed. HUMABIO Identity management is subject in **Chapter 5**. The chapter about risk assessment (**Chapter 6**) lists categories of risk and concludes that it is very important to take into account the prospective participants' view of the importance of risk. The end point of this process is the informed consent, given by the prospective participant. In **Chapter 7** a differentiation between therapeutic and non therapeutic research is given. In **Chapter 8**, deception and debriefing are picked out as central themes. In **Chapter 9** organization and insurance issues are described. A future steps part follows in **Chapter 10**, in which it is described how information on ethical issues is being collected and evaluated. The HUMABIO advisory board is listed in **Chapter 11**. Last but not least, recommendations follow in **Chapter 12**.

1 Introduction

1.1 Project description

HUMABIO is a STREP where new types of biometrics are combined with state of the art sensorial technologies in order to enhance security in a wide spectrum of applications.

Several shortcomings in biometric authentication will be addressed in the course of HUMABIO which will provide the basis for improving existing sensors, develop new algorithms, procedures and applications, towards creating an Ambient Intelligence Space in security sensitive, controlled environments with increased security requirements.

In particular, research will be focused on these issues: scientific/technological (such as biodynamic authenticating indicators and physiological state diagnosis); user-centred (such as acceptance, usability and legal framework); and application-related (such as continuous authentication, secure interoperable biometrics and emotional staging and monitoring).

Performance evaluation will be conducted throughout the whole project in a sound and statistically relevant way, under a specifically-created committee control. Significant efforts will be devoted to contributions to standards, co-operation with existing organizations (such as NoE), and to dissemination of the results.

HUMABIO activities include development of pilots in various scenarios (such as transportation safety and continuous authentication in controlled environments) for which important final users have already been involved. Other technological deployments will be made during the project lifetime, driven by the first successful research results; the participation of big industrial partners (with big customers) ensures a very large catchment area.

The project aims at developing a **modular, robust, multimodal biometric security authentication and monitoring system** which utilizes a biodynamic physiological profile, unique for each individual, and advancements of the state-of-the art in behavioural and other biometrics, such as facial, speech, gait recognition and seat based anthropometrics.

The objectives of the project are:

- Study of the authentication potential of dynamic physiological indicators, such as EEG and ECG features, blood pressure, blood oximetry, respiratory movements, etc. using event related responses analysis and standard measurements. Exploitation of very extensive databases made available by HUMABIO's partners that contain physiological measurements of thousands of healthy volunteers.
- Systematic research on the detection of baselines and criteria for the above indicators that exhibit sufficient intra-personal stability and inter-personal variations, in order to be used for continuous authentication. This research will add upon existing research that has demonstrated the strong authentication potential of emerging biometrics such as EEG and ECG, but has not yet led to exploitable products.
- Creation of a human physiological profile template. Fused physiological measurements will develop a unique physiological signature of the individual.
- Study of the physiological responses of various abnormal emotional states. Definition of criteria and thresholds, classification of various extreme emotional states and correlation to the variance of physiological indicators.

- Development of advanced face, speaker and gait recognition modules. Development of an anthropometric authentication system based in seat sensors. The creation of an unobtrusive and transparent to the user, non-stop authentication system deriving from the fusion of these modules.- Development of multimodal fusing algorithms for the creation of robust multi-biometric authentication systems based on physiological and behaviour related biometrics.
- Development of embedded connectivity at the body (Body Area Network), the local (Local Area Network) and the wider (Wide Area Network) area, to guarantee the secure, wireless, low-cost and high-speed operation of all sensors and systems that are utilized.
- Development of innovative signal processing and computational intelligence algorithms for data fusion, data management, sensor integration and power consumption minimisation.
- Development of the appropriate secure and updateable biometric template database for the authentication and monitoring of the individuals in controlled and security sensitive environments.

The final objective of the project will be the development of a multi-sensorial system for the authentication of the identity of the subject, the validation of his/her capacity to perform his/her tasks and the continuous assessment and monitoring of the physiological and emotional state. Main properties but also specificity of such platform will be:

- ***autonomous***: that means to be able to provide automatically a positive authentication and a diagnosis about the subject's state.
- ***non-supervised***: that means that interpretation of the diagnosis must be performed by an intelligent decision making module and this information should be displayed to the proper authority without any on-line intervention of an expert.
- ***non-obtrusive***: this excludes all wired sensors.

1.1.1 EU Ethical Guidelines

Ethical recommendations and guidelines related to the EU Framework Programme 6 will be followed by the consortium. The guidelines that apply in particular to HUMABIO relate to the use of personal information and biotechnology. They could be summarised as follows

- A detailed description of the procedure for obtaining informed consent is needed
- Protection guidelines for the confidentiality of such personal data have to be specified
- A specific consent should be given to the access of the stored data. With whom are the data shared (with which stakeholders).
- Applicants should also describe the process of encoding or anonymisation used and indicate if the collected data will be used for commercial purposes.
- Even where only anonymised data are used adequate security measures for storage and handling of such data must be shown”¹

¹ http://europa.eu.int/comm/research/science-society/ethics/rules_en.html#ethical

The amount of information, guidelines and Directives concerning ethical issues offered by the EU for the scientific research is multifaceted. An overview can be found at http://europa.eu.int/comm/research/science-society/page_en.cfm?id=2995. The primary concerns of these Ethical guidelines are medical, human and genetic research. However there are also guidelines relating to personal data, and this has a bearing on the HUMABIO project.

1.1.2 Legislation of the European Commission

The Ethics considered are for the development of the project, and not for the eventual use of the system. Ethics can be defined as ‘a system of principles governing morality and acceptable conduct’¹ or ‘the study of fundamental principles that defines values and determines moral duty and obligation’². However in this context a wider and more specific definition is required. Specifically, the rights that are protected need to be identified, as well as the reasons why they are protected.

¹ <http://wordnet.princeton.edu/perl/webwn?s=ethics>

² www.science.psu.edu/alert/frontiers/Glossary1-2001.htm

The ethical guidelines are written in accordance with EU legislation:

- The **Charter of Fundamental Rights** of the EU (dignity, freedoms, equality, solidarity, citizen’s rights, justice, general provisions)
- **World Medical Association Ethics** guidelines
- **Directive 2001/20/EC** of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use. This might apply to some of the EEG and ECG devices and related measurements within HUMABIO.

- **Directive 95/46/EC** 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 on the free movement of such data
 - **Directive 2002/58/EC** concerning the processing of personal data and the protection of privacy in the electronic communications sector
 - **Council Directive 83/570/EEC** of 26 October 1983 amending Directives 65/65/EEC, 75/318/EEC and 75/319/EEC on the approximation laid down by law, regulation or administrative action relating to proprietary medicinal products
 - **Directive 98/44/EC** of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions
 - **Directive 99/5/EC** on Radio Equipment, Telecommunications Terminal Equipment and the Mutual Recognition of Their Conformity. Access to control devices and control is a key issue from the viewpoint of the person
 - **Directive 2001/95/EEC** includes the general safety requirements for manufactures and distributors. The manufacturers must put on the market products that comply with the general safety requirement. They must also provide consumers with necessary information
 - **Low Voltage directive (LVD) 73/23/EEC** seeks to ensure that electrical equipment within certain voltage limits provides a high level of protection
 - **Directive 90/219/EEC** on the contained use of genetically modified micro organisms
 - **Directive 2001/18/EC** of the European Parliament and of the Council of 12 March 2001 on the deliberate release into the environment of genetically modified organisms and repealing Council Directive 90/220/EEC
- The last two directives do in all likelihood not concern research as it is foreseen in HUMABIO.

1.1.3 International conventions and declarations

We respect the following international conventions and declarations:

- **Helsinki Declaration**, lastly amended in Tokyo 2004.
- **Convention of the Council of Europe on Human Rights and Biomedicine** signed in Oviedo on 4 April 1997, and the Additional Protocol on the Prohibition of Cloning Human Beings signed in Paris on 12 January 1998.
- **UN Convention on the Rights of the Child**, 2002.
- **Universal Declaration on the human genome and human rights adopted by UNESCO**, 1997.

We also take into account to the opinions of the **European Group of Advisers on the Ethical Implications of Biotechnology** (1991 -1997) and the opinions of the **European Group on Ethics in Science and New technologies** (as from 1998).

The World Medical Association specified guidelines for medical research which can be applied to HUMABIO, even though the applications are technical and social rather than medical. These suggestions must be seen in addition, even though they are not specifically referred to in Framework Programme 6.

The main ethical considerations for medical research are:

- Scientific Merit
- Social Value
- Risks and Benefits

- Informed Consent
- Confidentiality
- Honest reporting of results.¹

¹
<http://www.wma.net/e/ethicsunit/resources.htm>

1.2 Pilot setup

(DoW page 51 et seq.)

In the next paragraphs the pilot plans will be introduced and the risks of misuse of the developed technologies and procedures for personal privacy or autonomy at work will be identified and evaluated. If applicable, mitigation strategies against them will be suggested.

As described in the DoW the pilots for the evaluation of the system are designed in a way to cover the objective of the project, which is the reliable authentication of individuals in controlled environments and the emotional state diagnosis of operators in critical tasks, in order to prevent human operator related accidents. Three applications are considered in order to highlight the modalities of HUMABIO and its adaptability to different application scenarios.

- a truck, representing in general the transport means environment,
- an office environment, for resources protection from unauthorized access and for the evaluation of the system as an emotional state classifier,
- an airport, for non-stop and unobtrusive authentication of employees in the controlled area.

The following table correlates the applications to the HUMABIO platform configurations, in order to show the multimodality of the system and the different parameters which will be measured:

	Mobility		Physiological biometrics				Behavioural and other biometrics				Operation mode				
	FS	M	EEG		ECG	BL	F	S	Vo		G	V	A	M	
			ERP	Base					D	Fr	C	W			
Operation mode															
Validation	x		x		x	?	x		x		x	?			
Authentication	x	x		x	x	x	x	x		x	x	?			
Monitoring	x			x	x	x				x					
Environment															
Truck	x		?	x	x	x	x	x					?	x	x
Office	x		?	x	x	x	x	x		x			?	x	x
Airport		x		?			x	x		x	x	?		x	

FS	Fixed seat
M	Moving freely
BL	Blood pressure related parameters
F	Face biometrics
S	Sensing seat biometrics
Vo	Voice biometrics
G	Gait biometrics
V	Validation
A	Authentication
M	Monitoring
Base	Baseline
D	Dictated – text dependent
Fr	Free speech
C	Camera based
W	Using wearable sensors
?	Not certain applicability, depending on the scenario, the acceptable obtrusiveness level and other parameters deriving from WP1 requirements.

Table 1: HUMABIO Application

The project will develop a biometric authentication core (BAC) that will be tailored for each pilot. The core architecture comprises:

- The integration of BioSec API at the client-side. It will also include the description of the common data formats based on the ISO/IEC JTC/1 SC37 data interchange framework (ISO/IEC JTC 1/SC 37, WG2, SD 19785 CBEFF – Common Biometric Exchange Formats Framework)
- An authentication protocol based on the Extensible Authentication Protocol (EAP) (Aboba, B., L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz, Ed., Extensible Authentication Protocol (EAP), RFC 3748, June 2004). The authentication protocol will be a transport layer, so the biometric data and other authentication parameters will be securely **transmitted between server and client**; Palekar, A., et al., Protected EAP Protocol (PEAP July 2004)
- At the server-side BioSec API will be the interface for the fusion and matching algorithms.

In this way, the implementation of the three pilots will be a template adaptation to each scenario features. Early specification of the interfaces will allow for early development of the BAC, and it will facilitate an iterative refinement process of the core during the project life.

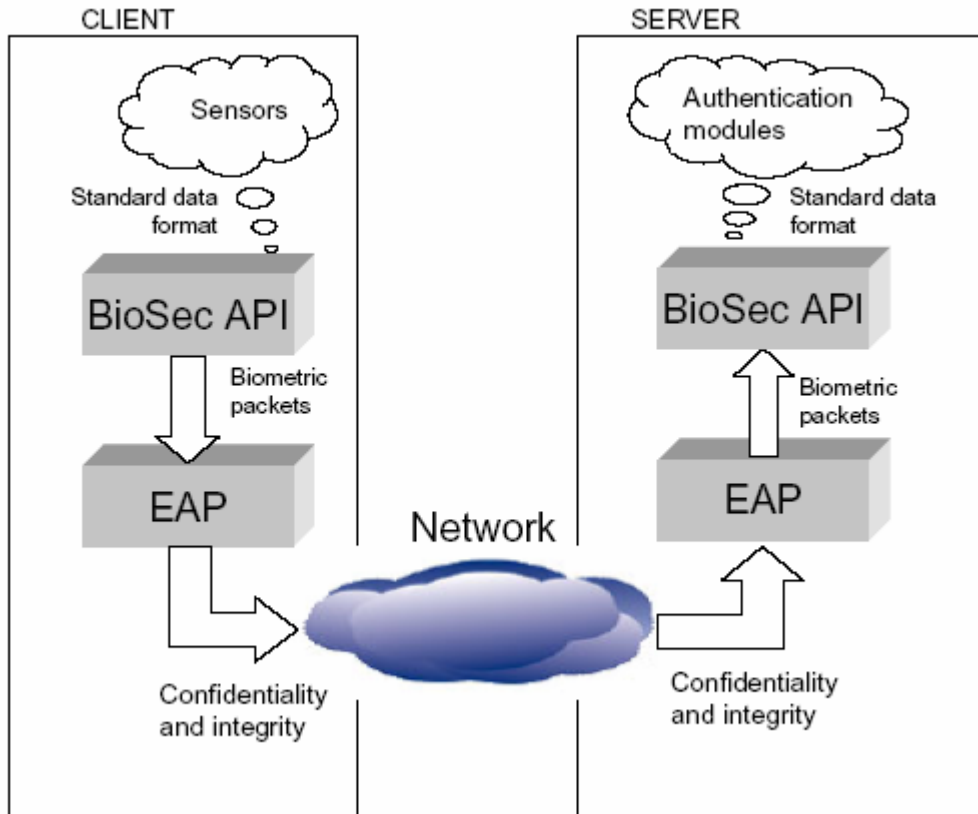


Figure 1: HUMABIO Biometric Authentication Core for the pilots

Description of pilots:

- passages relevant to ethical issues are written in **bold** and *italics*

- Truck (driver authentication)

In this application scenario HUMABIO will be installed in a vehicle (truck in this case), in order to *authenticate the driver*. Volvo will provide the vehicle and its facilities in Gothenburg for the implementation of the pilot. The application targets primarily professional drivers and transport companies. In this category we can classify money transfer vehicles, security company vehicles, mass transportation vehicles, such as buses, trains and airplanes, and also heavy equipment machinery, such as cranes. Since this application concerns professional drivers and operators, the use of minimally obtrusive *sensorial equipment* in the form of *hats, belts or wrist bands* can be considered to be acceptable by the subject, however this will be defined by the findings of WP1 concerning user requirements and acceptance. In addition the nature of the application environment, which is confined with the subject operating seated in a fixed seat, allows the use of *physiological measurements* in order to create the *operator's physiological profile*. In that way, this application is very suitable for the testing of HUMABIO's biodynamic indicators as the system's main *biometric authenticator*. The *face and speaker recognition techniques* will function in parallel with the physiological authenticator, in order to increase the system's reliability. *The measurements from the various sensors will be transmitted wirelessly to the Personal Data Processing*

Unit PDPU, which will be miniaturized, integrated in clothing e.g. in a belt. The PDPU (Personal Data Processing Unit) will function as a wireless transmission bridge and forward the integrated physiological measurements to the HUMABIO authentication and *monitoring module* which *will decide* on the positive identification of the driver and classify *his/her emotional state*. In case there is a problem either with the identity of the driver or his/her state the module will *notify* the *proper authorities* through the *WAN* gateway.

The secondary objective of this application will be the detection of *abnormal physiological states* that could potentially lead to poor performance and accident-prone situations. The sensorial infrastructure that will be installed in the vehicle and the driver clothing will provide the measurements and means to *detect drowsiness and sleep* among other dangerous states providing a framework for safe driving.

Ethical phrase	Ethical field	Law/directive	Relevant chapter in this manual
<i>authenticate the driver</i>	Informed Consent Privacy, Data protection	Charter of Fundamental Rights, World Medical Association Ethics	2, 3, 4, 5
<i>sensorial equipment</i>	Biocompatibility	Council Directive 83/570/EEC, Directive 98/44/EC Low Voltage directive (LVD) 73/23/EEC	Project summary
<i>physiological measurements</i>	Biocompatibility Informed Consent, Data Protection, Privacy, Confidentiality	Directive 95/46/EC, Directive 2002/58/EC World Medical Association Ethics	2, 3, 4, 5, Project summary
<i>Operator's physiological profile</i>	Privacy, Data Protection, Confidentiality	Charter of Fundamental Rights World Medical Association Ethics	3, 4, 5
<i>biometric authenticator</i>	Privacy, Data protection, Confidentiality	Charter of Fundamental Rights Directive 95/46/EC, Directive 2002/58/EC World Medical Association Ethics	3, 4, 5
<i>face and speaker recognition techniques</i>	Privacy, data protection, Confidentiality	World Medical Association Ethics	3, 4, 5
<i>The measurements from the various sensors will be transmitted</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Directive 95/46/EC, Directive 2002/58/EC World Medical Association Ethics	2, 3, 4, 5

<i>wirelessly to the Personal Data Processing Unit</i>		Directive 99/5/EC	
<i>monitoring module will decide</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Directive 95/46/EC, Directive 2002/58/EC	2, 3, 4, 5
<i>his/her emotional state</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5
		World Medical Association Ethics	
<i>notify the proper authorities</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5
WAN	Security Issue	Directive 95/46/EC, Directive 2002/58/EC	3, 5
		Directive 99/5/EC	
<i>abnormal physiological states</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5
		World Medical Association Ethics	
<i>detect drowsiness and sleep</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5
		World Medical Association Ethics	

Table 2: Ethical issues in the truck pilot

- Office/Laboratory (authentication + emotional staging)

The Lab Innovation Center of Fraunhofer will provide their new facilities for the implementation of the office/lab pilot. The Lab Innovation Center is a research and development platform of Industry and public authorities, where innovative work environments in combination with cutting-edge equipment for *bio/nano research* are investigated and further developed. Highest requirements to safety and access authorization make the Fraunhofer Lab Innovation Center an ideal test bed for most applications developed within HUMABIO. In this context, the primary aim of HUMABIO in this pilot is the *authentication of the computer and lab-systems operators* in order to minimize the risk of unauthorised data access. For this matter especially the interaction of distributed networking laboratories and the external access to lab-data and the (telematic supported) controlling of specific lab equipment such as a *FACS* (Fluorescence Activated Cell Sorter) are in need for high-security measures. The secondary aim of HUMABIO is *the detection of extreme emotional and abnormal physiological states* that could hinder attention and efficiency during the performance of critical tasks. Such a system could be applied to banks, military

installations, research labs, R&D utilities and in general in controlled environments where there is need to protect data and resources. The advantage of HUMABIO over current security solutions is the *continuous authentication* of the user, using *biometric features* that are not external (such as a fingerprint or the face) and thus harder to copy. In that way the risk of system spoofing is minimized. For the authentication mode of HUMABIO both *physiological and behavioural biometrics* can be used and function in parallel, while the final decision will take place by the late fusion (or decision level fusion) of the two authentication modules. *Face and speaker biometrics* will add to the robustness of the system and dependability on its decision. The implementation concept is similar to the one for the truck application shown in Figure 2.

- Subjects will be *wearing the physiological sensors* and will be *authenticated by the system*. If the subject moves away from his/her workstation, the workstation will be locked.
- Individuals will be driven to *experience extreme emotional states* (these will be defined in WP2) and maybe inattention. The system should be able to classify the state, discriminate this situation from false authentication and identification and take some kind of action, for example set the operation to autopilot, notify authorities, etc.

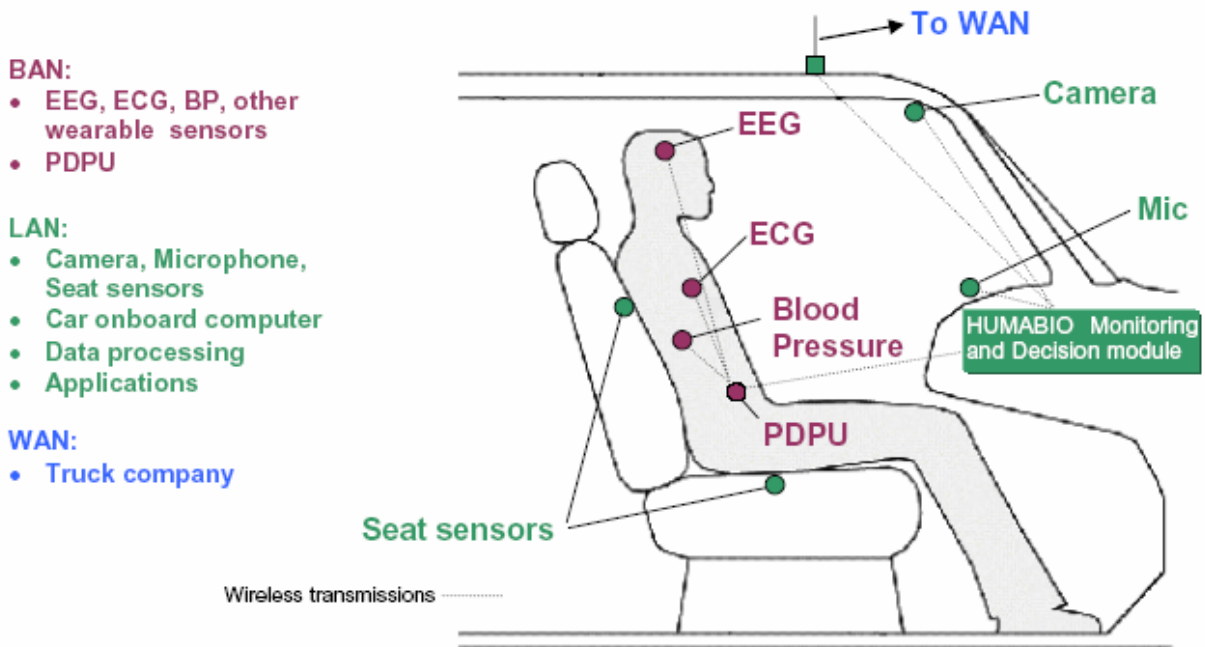


Figure 2: HUMABIO Concept for vehicle application

Ethical phrase	Ethical field	Law/directive	Relevant chapter in this manual
<i>bio/nano research</i>	Biocompatibility, Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics Directive 2001/95/EEC Directive 2001/20/EEC	2, 3, 4, 5

<i>authentication of the computer and lab-systems operators</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5, 9
		Directive 2001/95/EEC	
		Directive 99/5/EC	
<i>FACS</i> (Fluorescence Activated Cell Sorter)	Biocompatibility	World Medical Association Ethics	Project summary
<i>the detection of extreme emotional and abnormal physiological states</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights, Directive 95/46/EC, Directive 2002/58/EC	8 “Deception & Debriefing”
<i>continuous authentication</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5
		Directive 99/5/EC	
<i>biometric features, physiological and behavioural biometrics, Face and speaker biometrics</i>	Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics	2, 3, 4, 5
		Directive 2001/20/EEC	
<i>wearing the physiological sensors</i>	Biocompatibility, Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics	2, 3, 4, 5, Project summary
		Low Voltage directive (LVD) 73/23/EEC	
		Directive 2001/95/EEC	
		Directive 2001/20/EEC	

Table 3: Ethical issues in the office application

- Restricted area pilot

The system will be installed in a controlled area in Euroairport in Basel, Switzerland. The aim is to *authenticate the identity* of authorized employees that can move freely in the area. Depending on the acceptable *obtrusiveness level*, which will derive from the findings of WP1, the appropriate sensor setup will be utilized. Two possible obtrusiveness scenarios are considered: the *totally unobtrusive scenario*, which dictates that the employees will not carry any sensor on them, which in turn means that the physiological profile of the subject will not be available and the partially obtrusive scenario in which *wireless wearable sensors* and the utilization of the *physiological indicators* will be included. The sensors that will be used in the first scenario are the camera and possibly a microphone. The subject will carry *an ID in the form of RFID* and the authentication will take place using the *exclusively the*

behavioural profile which will comprise of the *gait, face and speaker recognition* modules, whenever applicable. The whole process will be transparent to the subject since the authentication process will not require from the subject to execute specific tasks.

The sensors that will be used in the second scenario are the ones in the previous scenario with the addition of *wearable sensors and the personal PDPU*. In this case, the physiological profile will also be available and additional information such as the physiological state of the subject could be extracted, in order to *assess his or her capacity to perform his/her task*.

Ethical phrase	Ethical field	Law/directive	Relevant chapter in this manual
<i>authenticate the identity</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights, World Medical Association Ethics Directive 2001/20/EEC	2, 3, 4, 5
<i>obtrusiveness level</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Directive 95/46/EC, Directive 2002/58/EC	2, 3, 4, 5
<i>totally unobtrusive scenario</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Directive 95/46/EC, Directive 2002/58/EC	2, 3, 4, 5
<i>wireless wearable sensors</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Directive 2001/95/EEC Low Voltage directive (LVD) 73/23/EEC	2, 3, 4, 5
<i>physiological indicators</i>	Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics Directive 2001/20/EEC	2, 3, 4, 5
<i>an ID in the form of RFID</i>	Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics Directive 99/5/EC Directive 95/46/EC, Directive 2002/58/EC	2, 3, 4, 5
<i>exclusively the behavioural profile</i>	Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics Directive 2001/20/EEC	2, 3, 4, 5
<i>gait, face and speaker recognition</i>	Informed Consent, Data Protection, Privacy, Confidentiality	World Medical Association Ethics Directive 2001/20/EEC	2, 3, 4, 5
<i>the personal PDPU</i>	Data Protection	Directive 95/46/EC, Directive 2002/58/EC	3, 4

<i>assess his or her capacity to perform his/her task</i>	Informed Consent, Data Protection, Privacy, Confidentiality	Charter of Fundamental Rights	2, 3, 4, 5
		World Medical Association Ethics	
		Directive 2001/20/EEC	

Table 4: Ethical Issues for restricted area pilot

Single studies conducted by Starlab and Forenap which are not officially stated as Pilot setups but who will conduct EEG and ERP experiments will follow the same ethical principles as the Pilots.

Summarising the general objectives of the pilots on an abstract level, HUMABIO aims to enhance security at supervised and controlled environments. The project research revolves the biometric **Authentication** that describes the internal physiology of the subject and the **Validation** and **Monitoring** during critical operations. The following table describes the way the system proposes these three main operation phases.

Phase	State	Methods	Application
Authentication	Initial	<ul style="list-style-type: none"> - Password - RFID-token - Face recognition - Text dependent voice verification - Event related potentials (EEG, ECG, other) 	<ul style="list-style-type: none"> - When the subject logs into the protected system - Before validation phase
	Continuous	<ul style="list-style-type: none"> - EEG baseline - ECG features - Other physiological features - Face authentication - Speaker verification (free speech analysis) 	<ul style="list-style-type: none"> - Continuously while the subject performs his/her tasks or accesses a protected resource
	Non-obtrusive	<ul style="list-style-type: none"> - RFID-token - Face authentication - Gait authentication - EEG baseline - Other physiological signatures 	<ul style="list-style-type: none"> - When the subject accesses a protected area and is able to move freely
Validation of initial 'nominal' state		<ul style="list-style-type: none"> - Event related potentials - ECG analysis - Voice analysis - Equilibrium analysis - Analysis of other physiological measurements 	<ul style="list-style-type: none"> - Before the subject commences his/her tasks
Monitoring		<ul style="list-style-type: none"> - EEG features - ECG features - Other physiological features - Speaker verification (free speech analysis) 	<ul style="list-style-type: none"> - Continuously, while the subject performs his/her tasks

Table 5: General Objectives of HUMABIO

1.3 The T1.3 Template on ethical and legal issues

This Manual provides background information on the different questions and subsections used in T1.3 “template on ethical and legal issues”. Within this Ethics manual, the content of this template will be also justified on scientific and legal basis in depth.

The questionnaire on ethical and legal issues has to be filled in by the investigator who conducts experiments. It is also a sort of preliminary checklist, in which the researcher is reminded to take into account all the relevant ethical aspects before conducting any experiment. As experience in previous projects has shown, it is very difficult for the partners and the feedback is very low at this early stage of the project. The final version of the questionnaire on ethical and legal issues will be divided into different subsections (informed consent, ethical control instruments, privacy, safety, risk assessment).

The questionnaire on ethical and legal issues will be filled in by all partners who are planning to conduct experiments. Here the results will be reviewed by the ETHICS ADVISORY BOARD and summarized in the Ethics Manual and the Controlling report.

Informed consent documents will be annexed to the questionnaire. **With the aid of those, the informed consent will be also documented; see also chapter *Informed consent*.** The informed consent documents will be used as material when the trials start and will eventually be slightly modified and completed until then.

The purpose of the section ‘organizational and insurance issues’, is to highlight the organizational and any applicable insurance issues that the partners should introduce within the ethical code of the project. In this context, organizational issues, like accessibility of facilities and services and different reimbursement schemes (legal basis for reimbursement, amount and type of payment, insurance provision) for test/end-users involved as interviewees in research, are addressed at the questionnaire section for organizational and insurance issues, will be annexed to this document.

2 Informed consent

UNESCO directive, 1997: Universal Declaration on the human Genome and Human Rights:

The right of each individual according to article 5 B b) & c) of the UNESCO Declaration (UNESCO 1997) to decide whether or not to be informed of the results of any medical, physical or genetic examination and the resulting consequences, if any, will be respected in full.

“B. RIGHTS OF THE PERSONS CONCERNED

Article 5 b): In all cases, the prior, free and informed consent of the person concerned shall be obtained. If the latter is not in a position to consent, consent or authorization shall be obtained in the manner prescribed by law, guided by the person's best interest. “

Article 5 c) The right of each individual to decide whether to be informed or not on the results of genetic examination and the resulting consequences should be respected. “

Every volunteer participating in the HUMABIO project needs to be fully aware of what they have been asked to do. This will be accomplished through training in the use of the HUMABIO tools and through the use of the informed consent form. Informed consent is the process by which a participant will be fully informed about the research in which he/she is going to participate. It originates from the legal and ethical right the participant has to direct what happens to his / her body and personal data and from the ethical duty of the investigator to involve the participant in research. Seeking the consent of an individual to participate in research reflects the right of an individual to self-determination and also his/her fundamental right to be free from bodily interference whether physical or psychological and to protect his / her personal data. These are ethical principles recognised by Law as legal rights. A distinction between three informed consent elements is possible: the information given, the capacity to understand it and the voluntariness of any decision taken.

Respect for persons requires that participants, to the degree they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided, when adequate standards for informed consent are satisfied.

The written information as well as the sought informed consent corresponds to information gathered from the revised version of the *Helsinki Declaration* of 1964, as lastly amended in Tokyo, 2004, and the Convention of the Council of Europe on Human Rights and Biomedicine (1997).

2.1 Participant groups and their consent

Whether a person has the capacity to understand the information depends on the ability to comprehend the nature and purpose of any course of action and the short and long-term risks and benefits of what is proposed.

Informed Consent is crucial in all aspects of social research and particular attention will be given when disabled people are involved that rights are protected and compliance is always freely entered into (which will most likely not be the case in HUMABIO as only healthy subjects will be tested). Information that will affect the respondent's willingness to participate will always be provided in appropriate accessible formats and never be deliberately withheld. Potential participants will also not be overwhelmed with unnecessary information.

For those unable to read the consent form (blind and partially sighted, dyslexic, illiterate) an ordinary documentation of informed consent is also not appropriate. For these people the information will be provided in appropriate alternative media (e. g. large print, audio tape, Braille).

2.2 Basic elements of informed consent

In all cases, the prior, free and informed consent of the person concerned will be obtained. If the respective participant is not in a position to consent due to the most sensitive nature of the HUMABIO project she or he will be excluded from any laboratory-based experiments, feasibility studies and pilots of the project. So it will be strictly monitored, that within the context of the HUMABIO research none of the partners involved will obtain consent or authorization for participants not being able to give this consent for themselves from a relative, legal counsellor or legal guide. Adherence to this regulation is mandatory, even if such an indirect consent would be guided by the person's best interest and be allowed under the respective national and European laws.

In order to involve a human being as a participant in research, the investigator will obtain the legally effective informed consent of the participant or the participant's legally authorized representative. All investigators within HUMABIO will seek such consent only under circumstances that provide the prospective participant or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence. The information that is given to the participant or the representative will be in a language understandable to the participant or the representative. No informed consent, whether oral or written, may include any exculpatory language through which the participant or the representative is made to waive or appear to waive any of the participant's legal rights, or releases or appears to release the investigator, the sponsor, the institution or its agents from liability for negligence. In seeking informed consent according to the American Psychological Association (2002), the following information shall be provided to each participant:

1. the purpose of the research, expected duration, and procedures;
2. the possible risks, discomfort, adverse effects, and side-effects (if any);
3. a description of any benefits to the participant or to others which may reasonably be expected from the research;
4. explanations on confidentiality (and limits) of the data;
5. their right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing;
6. whom to contact for questions about the research and research participants rights.

In addition:

- a. Appropriate insurance or indemnity to cover the participant in trial should be provided.
- b. A table of certified sensors and/or software (medical device in general) as well as the prototypes not yet certified that shall be used by the patient underlying the potential risks and legal binds that may be in effect should be also provided.

When appropriate, one or more of the following elements of information shall also be provided to each participant:

- (1) a statement that the particular procedure may involve risks to the participant (or to the embryo or fetus, if the participant is or may become pregnant) which are currently unforeseeable (the case being very unlikely within HUMABIO);
- (2) anticipated circumstances under which the participant's participation may be terminated by the investigator without regard to the participant's consent;
- (3) any additional costs to the participant that may result from participation in the research (not expected to be the case within HUMABIO);
- (4) the consequences of a participant's decision to withdraw from the research and procedures for orderly termination of participation by the participant;
- (5) a statement that significant new findings developed during the course of the research which may relate to the participant's willingness to continue participation will be provided to the participant; and
- (6) the approximate number of participants involved in the study.

2.3 Guidelines for compiling the informed consent form

The following comments may help investigators how to provide information to prospective participants and therefore obtain consent:

- Informed consent is a *process*, not just a form. Information should be presented to enable persons to voluntarily decide whether or not to participate at research.
- It is a fundamental mechanism to *ensure respect for persons* through provision of thoughtful consent for a voluntary act. The procedures used in obtaining informed consent are designed to educate the participant population in terms that they can understand. Therefore, informed consent language and its documentation (especially explanation of the study's purpose, duration, experimental procedures, alternatives, risks, and benefits) must be written in "layman's language", (i.e. understandable by the people being asked to participate). The written presentation of information is used to document the basis for consent and for the participants' future reference. The consent document will be revised when deficiencies are noted or when additional information will improve the consent process.
- The investigator should be aware of the fact that the use of the first person (e.g., "I understand that ...") can be interpreted as suggestive, may be relied upon as a substitute for sufficient factual information, and can constitute coercive influence over a participant.
- Use of scientific jargon and legalese is not appropriate. The document is primarily thought of as a teaching tool not as a legal instrument.
- *The overall experience* that will be encountered is described.

- The human participants will be informed of the reasonably foreseeable harms, discomforts, inconveniences and risks that are associated with the research activity. If additional risks are identified during the course of the research, the consent process and documentation will be revised to inform participants as they are re-contacted or newly contacted.
- **The benefits** that participants may reasonably expect to encounter will be described. There may be none other than a sense of helping the public at large. If payment is given to defray the incurred expense for participation, it must not be coercive in amount or method of distribution.
- The participants are told the extent to which their **personally identifiable private information** will be held in confidence. See also the **chapter 4** about *privacy of individual data*.
- If **research-related injury** (i.e. physical, psychological, social, financial, or otherwise) is possible in research that is more than minimal risk, an explanation will be given of whatever voluntary compensation and treatment will be provided (not expected to be the case within HUMABIO).
- **The legal rights of participants will not be waived in any way.** The participants should not be given the impression that they have agreed to and are without recourse to seek satisfaction beyond the institution's voluntarily chosen limits.
- **Details of contact persons** who are able to answer questions of participants about research, rights as a research participant, and research-related injuries will be provided.

A single person is not likely to be appropriate to answer questions in all areas. This is because of potential conflicts of interest or the appearance of such. Questions about the research are most often best answered by the investigator(s). However, questions about the rights of research participants or research-related injuries (where applicable) may best be answered by the on-site doctor for instance. These questions can also be addressed to the investigator, an ombudsman, an ethics committee, or other informed administrative body. The informed consent document will contain contact information with local telephone numbers to answer questions in specified areas.

- The participation is **voluntary** and the participant has the **right to withdraw at any time**. It is important to point out that no penalty or loss of benefits will occur as a result of either not participating or withdrawing at any time of the experiment.

A so-called “two part consent” will be used; this term means that in a first step the participant is being asked to give informed consent to the specific experiment of HUMABIO. In a second step consent and research for storage and future research will be asked and documented separately. Both consents can be included in one form (containing both the information about HUMABIO related issues and the possibility of using the data for future research).

It will be the responsibility of the partner conducting the respective research to ensure that all uses of data/samples are in accordance with the consent obtained from the participant.

The HUMABIO user groups do not include mentally disabled people (people unable to give a valid consent); only people with limited learning or cognition (i.e. memory or concentration or divided attention) difficulties, i.e. due to normal ageing. Any person not able to give a valid informed consent must be excluded from HUMABIO tests.

2.4 Informed consent and those unable to read the form

There are a range of people who are unable to read the consent form; these include those who have a severe visual problem, those with severe dyslexia, those who are illiterate and those whose knowledge of the language may be limited (e.g. a recent immigrant). For these people the information will be provided in appropriate alternative media (e.g. large print, audio tape, Braille, through translator, etc.).

Informed Consent and the illiterate

Directive 2001 / 20 / EC of the European parliament and of the council states that in accordance with Article 3:

A clinical trial may be undertaken only if, in particular:

d) if the individual is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation.

2.5 The legal positions

The HUMABIO research does not include any treatments. The only relevant legal issue is the handling and protection of private data and their maintenance.

Analyzed material

- Use of human tissue

From the foreseeable course of the HUMABIO project human tissue will not be used. If the need of using human tissue for validating newly developed biometric measurement instruments or procedures should arise during the course of HUMABIO, small samples of saliva (stress hormones) and/or blood might be used. This would require the storage of these samples for the duration of the project and for a specified period of time after the end of the project if the respective national law of the institution where the samples are obtained, analyzed and stored does make such an extended storage period mandatory. In all other cases samples will

be destroyed immediately after final analysis. The participants will be informed about these procedures within the informed consent. The data will strictly be held confidential.

- Use of animals

Tests involving animal research will not be performed during HUMABIO.

Research in cooperation with developing countries

Within HUMABIO no research will be conducted in developing countries.

2.6 Documentation of informed consent

Informed consent shall be documented by the use of a written consent form approved by the HUMABIO Ethics Advisory Board and signed by the participant (or the participant's legally authorized representative- most likely not the case in HUMABIO). A copy shall be given to the person signing the form. The consent form shall be a written consent document that embodies the elements of informed consent required in the previous section. Templates are provided in the Annex of this document, under HUMABIO informed consent form template. Form 1 general information has to be filled in every case. The information under header 2 INFORMATION ON THE RESEARCH STUDY has to be provided to the participant in a appropriate modality.

Healthy and able bodied participant

In the case of an experiment with a *healthy and able bodied participant*, forms:

Research participant's identity

Will be filled in by the participant.

The original will be kept by the investigator; a copy will be given to the participant.

Participant Consent Form

Will be filled in by the participant.

The original will be kept by the investigator; a copy will be given to the participant.

Investigators' confirming statement

This part will be filled in by the investigator.

The original will be given to the participant; a copy will be kept by the investigator.

3 Security issues in HUMABIO

In accordance with the DoW the following steps for data security, coding and economization will be fulfilled:

- Security of data storage and handling

All data retrieved will be anonymously inserted in the database(s). The original records will be destroyed after that, if this is not forbidden by law of the country in which the data was obtained, stored and analyzed. If data will be collected and stored in a web portal, then it will be duly protected by commercial security of highest available quality. This software has to be approved by the HUMABIO Ethical committee / advisory board prior to implementation. Access to data will be password-protected (at least two-stepped) and granted only to authorised partners for data analysis, for example partners who work in a relevant Workpackage in HUMABIO that depends on the data in question. Access for data input or change will be also password-protected and reserved only for partners who collect and provide data. After data collection has ended, the data input or change will only be authorized by the Coordinator, upon written request by the relevant partner. The rights of adding data to the data pool in a database will be handled separately and independently from the rights of retrieving or even edit data in these databases.

- Coding and economization (see also next chapter)

As an absolute minimum anonymous made data will not contain any of the following, or codes for the following:

- Name, address, phone/fax. number(s), e-mail address, full postcode
- Any identifying reference numbers
- Photograph or names of relatives

With both linked and unlinked anonymous made data it is sometimes possible to deduce individual's identities through combinations of information. The most important identifiers are:

- The age, if a small sample size is taken; in this case there has to be compromised between scientific precision and the protection of the individual privacy.
- Rare disease or treatment, especially if an easily noticeable illness is involved.
- Partial post-code, or partial address.
- Place of treatment.
- Occupation or place of work that is/are quite unique and easily identifiable.
- Combinations of birth date, ethnicity, place of birth, and date of death.

Wherever possible these combinations of data should not be accessible to persons not necessarily involved in the respective research. If possible these potentially revealing information segments should be stored separately.

3.1 Introduction - the need for security

Under EU FP6, the ethical considerations that concerns HUMABIO is that of biotechnology, and data collection requirements for personal information. They are summarised on the official WebPages from the European Commission: “Ethics in EU projects, Ethical issues in EU research proposals – checklist, updated 08.11.2005”.

‘Use of personal data in bio-banking (including gene-banking)

Applicants should describe the procedure for obtaining informed consent of persons and describe the arrangements for protecting the confidentiality of their personal data. Applicants should describe measures taken to encode or anonymise banked biomaterial (including traceability measures). Even where only anonymised data are used, adequate security for storage and handling of such data must be shown.’

‘Protection of personal data

Applicants should describe the procedure for obtaining informed consent of persons and describe the procedures for protecting the confidentiality of such personal data. Where data are to be shared with other stakeholders the persons whose data are collected should give a specific consent. Applicants should also describe the process of encoding or anonymisation used and indicate if the collected data will be used for commercial purposes. Even where only anonymised data are used adequate security measures for storage and handling of such data must be shown.’

Thus, HUMABIO system handles sensitive information that should be protected. The provision of HUMABIO services requires a secure operational environment. Without an appropriate level of security in place, no such a system can be operational. Security is therefore an important issue for HUMABIO.

Different stages of security levels should be included in the HUMABIO system which includes judgment about the dangers associated with the system and the resource implications of various means of avoiding or minimizing those dangers. Several major questions arise including the integrity of the information, the confidentiality of the information (i.e. who should be allowed to see what and under what conditions) and the availability to legitimate users. Participants of the tests and pilots need to be made aware that their information derived from the testing of the project will be shared between the stakeholders in the project in order to meet the project objectives.

In order to answer those questions it is necessary to:

- Identify the specific security requirements / threats / vulnerabilities associated to the various categories of users and data types.
- Study the related technology available.
- Define an appropriate security policy for accessing the information.
- Study the impact of adding security on the availability / performance of the system.
- Propose the conceptual structure and specific measures required to improve the security of the system.

HUMABIO information system is designed to provide the required level of security efficiently. However, as often happens, the objectives can conflict with each other. For example, security interests can conflict with performance. This should not be surprising, since

measures to enforce security often increase the size or complexity of a computing system. Security interests may also reduce the ability of the system to provide data to users, by limiting certain queries that seem innocuous by themselves. Introducing security into HUMABIO system is therefore a balancing process between providing the desirable level of protection on the one hand and maintaining an adequate level of availability and performance, so that legitimate users have easy access to the data, on the other. This conflict will be dealt with in HUMABIO by asking the user oneself to decide upon the accepted level of functionality and security one desires.

3.2 The security issue

Networking and communication security issues arise when a multitude of different sensors interact with local or remote applications. Three different networks can be defined: the Body Area Network (BAN), the Local Area Network (LAN) and the Wide Area Network (WAN). Data security and privacy concerns are applicable at any levels: BAN LAN and WAN. It is widely accepted today that security is a basic requirement for the appropriate introduction and use of information and communication technologies. The increasing employment of advanced technologies makes information systems more efficient, yet more complex, posing new challenges to ensure the protection and confidentiality of data and their integrity and availability. The new technologies contribute to improving the efficiency and quality of services to the patient and they are valuable tools for their management. They create however new situations regarding security that should be dealt with in a thorough and convincing manner (Pangalos, 1997).

Current thinking in information systems security is that the issues centre on **confidentiality** (information is only disclosed to those users who are authorized to have access to it), **integrity** (information is modified only by those users who have the right to do so), and **availability** (information and other IT resources can be accessed by authorized users when needed). The risks of violating these three security principles cannot be reduced to zero. But a specific balance of risks and effectiveness has to be found in all application systems. The level of security that should be included in an information system involves therefore some judgement about the dangers associated with the system and the resource implications of various means of avoiding or minimizing those dangers (Pangalos, 1997).

The following general principles related to information systems security have been widely accepted today:

- a. The security considerations must take into account all system S/W and H/W that touches information flowing into, and out of, the system.
- b. Data integrity is a key requirement. The system must preserve the integrity of the data stored in it. The user must be able to trust the system to give back the same data that is put in the system and to permit data to be modified only by authorized users. The data should not be destroyed or altered either accidentally, as in a system crash, or maliciously, as in some unauthorized person modifying the data. At the very least, the user should know if the data was corrupted.
- c. Data should be available when needed. This implies system fault tolerance and redundancy in data, software and hardware. Inference and aggregation must be studied and controlled.
- d. Audit should be detailed enough to be useful and sufficient enough so as not to severely burden system performance.

- e. The aim should be at providing adequate level of secrecy (prevent disclosure) and yet preserving integrity and integrity controls (e.g. referential integrity).
- f. The prototypes should be of general purpose, commercial quality and, according to most proposers, relational systems. The relational system has been chosen because it is currently the model of preference in the commercial world.

The basic security requirements of HUMABIO system are not unlike the security requirements of other computing systems. The basic problems of integrity, access control, exclusion of spurious data, authentication of users, reliability, etc. have already been examined in various sources. The following is a list of such technical security requirements for the security of the HUMABIO system:

- Physical integrity, so that the data of the HUMABIO system is immune to physical problems, such as power failures, and so that it is possible to reconstruct e.g. a database if it is destroyed through a catastrophe.
- Logical integrity, so that the structure of the HUMABIO databases is preserved. With logical integrity, a modification to the value of one field does not affect other fields, for example.
- Element integrity, so that the data contained in each element is accurate.
- Access control, so that a user is allowed to access only authorized data and so that different users can be restricted to different modes of access (e.g., read or write).
- User authentication, in order to be sure that every user of the HUMABIO system is positively identified, both for the audit trail and for permission to access certain data.
- Availability, so that users can access the HUMABIO system in general and all the data for which they are authorized.
- Auditability, so that it will be possible to track who has accessed (or modified) the elements in the HUMABIO databases.

A detailed description of each of the above requirements for the HUMABIO system security can be found in (Pangalos, 1997).

In order to prevent random access and to assure data protection in accordance to national law it is assumed that the host providing the database and any participating hosts that access it are directly in a secure area. The database area should also be detached from the LAN through a firewall that restricts access to this secured part.

A transaction gateway will be the direct contact for all client requests. It is responsible for a limited access to certain types of information per user (client), for a client authentication and for the prevention of intrusion/tapping (by using well tried encryption methods).

3.3 Measures for Improving the Security in HUMABIO

In dealing with information security, we refer to the three concepts: confidentiality, integrity and availability. In HUMABIO we must address all security aspects. There are five steps that should be followed for developing HUMABIO security:

- Develop Information Security Policies and Standards
- Design the Information Security Architecture and Processes
- Implement Information Security Awareness and Training
- Implement Information Security Technologies and Products

- Auditing, Monitoring and Investigating

3.3.1 Develop Information Security Policies and Standards

Only be relying on the technical solutions for data protection is not sufficient to ensure its security. The key is to implement a culture of security and confidentiality. It has to be an interdisciplinary approach between all users. The development of policies must be strong enough to protect the system, yet flexible enough not to disrupt the user and negatively affect productivity. When developing the policy document, it is important to build it so that everyone in the system can read and understand it. Policies must include requirements for certain types of documents to be encrypted, the use of digital certificates to ensure authenticity of communications and mandating the use of physical security products while creating the biometric authentication core.

3.3.2 Design the Information Security Architecture and Processes

Once policies are in place, the system needs to define the overall processes by which the policies will be implemented, monitored and enforced. Policies become valueless if they cannot be enforced, and enforcement is not feasible without monitoring. There are a number of policy management applications available on the market. The system needs to tread a careful path on this issue, as it is important for the involved partners to understand the value of security.

3.3.3 Implement Information Security Awareness and Training

Once the architecture is in place, the next step is to raise awareness and train the users of the HUMABIO system. This is the next most important step after policy definition. The majority of security programs fail because users do not use the security products effectively, if at all. Only an awareness program and training can address this issue. The users need to understand why security is critical to the system, and what they do on a day-to-day basis can have serious consequences. The users need to be thoroughly trained on the new security applications, and their use of those applications needs to be monitored to ensure that policies are being adhered to. Only when security is adopted as part of how people utilize the HUMABIO system and services, will the threat to the system be reduced.

3.3.4 Implement Information Security Technologies and Products

Once the policies are in place, the HUMABIO system needs to look to define and procure the technologies that will make up the security architecture.

Security Protocols: The security protocols that should be in place in order to secure the communication channels. Our proposal concerning the security protocols is the use of the Secure Authentication Protocol (SAP). We propose the implementation of SAP between any communicating entities.

In the framework of HUMABIO for example WLAN security is a major issue. At the most basic level wireless security requires Authentication (that only authorized users have access the network) and Encryption (information passed on the network can be read only by the intended recipient and without tampering). Various possibilities exist in the new standards for

WLAN security regarding the authentication process. We suggest a simple and secure authentication protocol (SAP) which can be used in small to medium networks and can provide a simple authentication. Secure Authentication Protocol is simple to implement and provides authorization in addition to secure authentication.

Anti-virus: At the heart of any security architecture is a strong anti-virus product that includes automatic updates of definitions when the PC is connected to the server. This process must be automated, and should not require user intervention. One of the latest products should cover the application's needs for virus protection.

Personal Firewall: A personal firewall product is a necessity for the modern road warrior. Personal firewall products can be configured for dual-zone protection – leaving system access unrestricted while on the trusted local network, and providing tight security while on the untrusted Internet.

Encryption: Either file/folder or full disc. The only way to ensure that the data remains secure, even if the device is not is to encrypt the data on the PC. A product that also offers e-mail encryption provides enhanced security.

Virtual Private Network (VPN): All connections between the mobile host and the corporate network should take place over a VPN. This ensures that the communication channel remains secure.

Access Control: Current design and implementation of the HUMABIO application assumes that a specific user operates as the security administrator of his/her own data.

Physical Security: All the devices must be protected. This can be done by using hardware like locks and cables, or via software by using software products like Computrace, which, the moment the stolen computer is connected to a phone line or has access to the Internet, silently reports the PC's location to the Computrace Monitoring Centre.

3.3.5 Auditing, Monitoring and Investigating

During the pilot set-up the communication system shall be audited in order to validate security requirements. Hacking attacks shall be done in order to detect any security holes. The policies that are developed and the processes that are put in place to enforce them are only going to be effective if there are regular audits of the system. Monitoring of adherence to policy and investigation into non-compliance is required on a regular basis.

Understanding where the weaknesses in the system are is the best way to find measures to correct them. Above all, policies and processes need to be reviewed and updated on a regular basis. Policy should never be considered static.

Information security is a difficult subject to address when the devices in question are safely tucked away behind the corporate firewall. Once they move outside the corporate firewall, managing those devices becomes much more difficult.

4 Privacy (and transparency) issues in HUMABIO

In accordance with the DoW the following steps for Protection of personal data will be fulfilled:

- Confidentiality

Protection of personal data

- All data associated with an identifiable person will be held confidential
- All research using identifiable personal data that is not already in the public domain will need approval by a standing research ethics committee
- Personal data on subjects will be used in strictly confidential terms and will be published as statistics (anonymously) only
- Any information about an individual will be held confidential, regardless of how this data was obtained. Accidentally obtained data in the course of the HUMABIO project will be treated with confidentiality
- All personal information will be coded or made anonymous in full and at the earliest possible point in time during data processing
- Each individual entrusted with patient information is personally responsible for the decision about disclosing it. Personal information will only be handled by health professionals or staff with an equivalent duty of confidentiality
- The collected data will under no circumstances be used for commercial purposes

“Google’s recent announcement that it will begin to offer free emails accounts to users has come under fire as initial plans call for all emails to be scanned for keywords in order to better target the users for advertising purposes (World Privacy Forum, 2004).“ (Freeman, L. & Peace, A.) This quote underlies the necessity of facing privacy issues in Information Technologies as most “daily life users” lose track on which of their personal information will be stored, for how long and to whom it is accessible. In HUMABIO, the protection of the privacy of participants is a responsibility of all people involved in research with human participants. Privacy means that the participant can control the access to personal information; he/she decides who has access to the collected data in the future (Patry, 2001). Due to the principle of autonomy the participants have to be asked for their agreement (informed consent) before private information can be collected.

It should be also ensured that all the persons involved in research work, understand and respect the requirement for confidentiality. The participants should be informed about the confidentiality policy that is used in the research.

The privacy plays a role at different levels:

- Hints to or specific personal information of any participant in publications.

It should be prevented to reveal the *identity* of participants in research deliberately or inadvertently, without the expressed permission of the participants. With regard to HUMABIO the development of a biometric authentication core (BAC) is crucial to this issue.

Physiological as well as behavioural parameters will be gathered during the pilots and would allow a “360 degree – scanning” of the participants if the data won’t be anonymized.

- **Dissemination** of data among partners. It has to be clarified to the partners that no spread of information about the health level of the participant will take place (for example insurance companies, employer, etc.).

- **Access** to data.

Define and protect method of access, data formats, method of archiving (electronic and paper), including data handling, data analyses, and research communications.

Offer restricted access to privacy sensitive information within the organization of the partner.

- **Protection** of the privacy within the organization of volunteers (employers, etc.) throughout the whole process like, communications, data exchange, presentation of findings, etc.

Furthermore, the participants have to be able to control the dissemination of the collected data. The investigator is not allowed to circulate information without *anonymisation*. This means that only relevant attributes, i.e. gender, age, etc. are retained. ***The identity of the participants will not be stored within HUMABIO trials.***

While common law establishes some core principles, it does not specify when confidential information may be disclosed to others, in research. Individuals and organizations using confidential information have to take responsibility for deciding what is justified and acceptable on a case by case basis (Medical Research Council, 2000).

In the behavioural sciences, respect for privacy and confidentiality is a central concept in the conduct of ethical research with human participants. Difficulties with privacy issues can lead to difficulties in properly conducting research. If a participant perceives that his or her privacy is threatened this can lead to biased sampling, evasive and/or false responses, and many other impediments that can affect the validity of the results.

As already mentioned, protection of confidentiality implies informing the participants about what may be done with their data (i.e. data sharing). As databases are developed, confidentiality will become increasingly hard to maintain. Simple stripping of the participants name and its replacement with a code is no guarantee of complete confidentiality. Some of the information participants share is extremely personal and thus very sensitive. An informed consent must be signed. This document also commonly states that the confidentiality will be preserved and the data collected may be shared with other researchers. A question currently under debate among behavioural scientists is whether a consent form stating that personal data will not be shared precludes sharing of data even if identifying characteristics are removed. The removal of identifying information from data gathered on an individual may not be enough since identities can be reconstructed from disparate data sources. There are solutions to the challenge of maintaining confidentiality including substituting numerical identifiers for names, aggregating data so that the performance of individuals is not obtainable, encryption or layering data so that researchers who need identifying information can obtain it only after signing a legal document that requires honouring the confidentiality of individuals. Researchers who do not need identifying information can have free access to aggregated data.

Important question:

How can confidentiality and control access be provided?

Two possibilities:

- The confidential information can be removed.
- Access must be restricted in some ways. (Johnson & Sabourin, 2001).

4.1 General principles

'Privacy in Medical Research and Law' was a 5th framework funded project (PRIVIREAL, No. PL QLRT-2001- 00056) on the implementation of Directive 95/46/EC on data protection. In order to identify **national** implementation of the Directive 95/46/EC the authors (Beyleveld, Rouille, Twonend & Wright, 2004) give an excellent overview in "Implementation of the Data Protection Directive in Relation to Medical Research".

Personal information must be regarded as confidential. Normally custodian of a large research database or register must ensure they have each person's explicit consent to obtain, hold and use personal information. In most clinical research cases this could be implemented in practice.

1. All research using identifiable personal information, or using anonymised data which is not already in the public domain, must be approved by a Research Ethics Committee.
2. All personal data must be coded or anonymised as far as is possible and consistent with the needs of the study, and as early as possible in the data processing. Only personal identifiers that are essential should be held.
3. Each individual entrusted with personal information is personally responsible for their decisions about disclosing it. Health professionals disclosing information should in particular, ensure they are familiar with the advice of the General Medical Council on disclosures for research.
4. Researchers must ensure that personal information is handled only by health professionals or staff with an equivalent duty of confidentiality.
5. Principal investigators must take personal responsibility for ensuring that training, procedures, supervision, and data security arrangements are sufficient to prevent unauthorized breaches of confidentiality (Medical Research Council, 2000).

All the above principles will be fully respected within HUMABIO.

4.1.1 Overview about different confidentiality principles

The following table summaries the different national and international approaches about confidentiality principles. It was written in accordance with the CSAGS (Confidentiality and Security Advisory Group for Scotland) document on "Data protection/ Confidentiality Principles". It includes:

- Data protection Act (1998)
- UN Data protection Guidelines

- Memorandum and Statement of the Working Group on Telecommunications and Media of the International Conference of Data Protection Commissioners
- General Medical Council (GMC)
- USA Secretary of Health and Human Service

Data Protection Act (UK)	UN (1990)	Germany (1990, amended 1994)
Fair and Lawful Obtaining of Data	1. Principle of Lawfulness and Fairness	Only to be obtained directly from client, except if there is legal provision to use other sources or collection from client would result in disproportionate effort
Secondary Data Use (no further processing beyond original purpose)	3. Principle of Purpose-Specification	Written consent (clearly marked) to be obtained, except in scientific research under certain circumstances. If depersonalised data used, key should be stored separately
Amount of Data – only that necessary		
Accuracy – accurate and up to date	2. Principle of Accuracy	Incorrect data to be corrected – by note being made in record or other means. If correctness can not be established, data can be blocked
Length of storage		
Rights of data subjects	4. Principle of Interested-Person Access	Inalienable right of data access, except for reasons of national security or other third party rights Should be aware of reasons for data collection and storage
Fraud Prevention – measures to be in place	7. Principle of Data Security	
Export to Other Countries – not if inadequate safeguards there	9. Trans-Border Flows	No communication where suspected that other countries' arrangements incompatible with German law
	5. Principle of Non-Discrimination (i.e. data use to discriminate against people)	People working in DP must give undertaking to maintain confidentiality.
	6. Power to make exceptions (e.g. national security, public health etc)	Compensation for causing harm by public data-holding body
	8. Supervision and Sanctions	

General Medical Council	USA Secretary of Health and Human Services
Right to Confidentiality	Boundaries – health care purposes only
Need to protect Information	Security – info to be protected
Sharing Information with patients (on their condition)	Consumer Control – patients have access to records and can correct errors
Disclosure to others providing care – express consent not needed (patients must be aware of this); patients' wishes to be respected on this; persons receiving info must	Accountability - people misusing information can be punished

respect confidence	
Disclosure not for treatment – seek consent, anonymise data where possible. Express Consent must be sought if patient directly affected; where patient not directly affected, e.g. research express consent should be sought if practicable; patient to be informed in any case.	Public Responsibility – claims to privacy must be balanced by public responsibility to common good.
General Medical Council	USA Secretary of Health and Human Services
Disclosure to protect patients or others (against doctors, or patients who continue to drive, in case of serious crimes) is to relevant bodies acceptable	
Disclosure in case of patients incapable of giving consent	
Disclosure after a patient's death – confidentiality still applies	
Disclosure in connection with judicial or statutory proceedings is acceptable	

Table 6: National and International approaches about confidentiality principles

4.2 Anonymisation and Coding

Information should be anonymised so that individual identities can not be revealed. Anonymisation provides a safeguard against accidental or mischievous release of confidential information.

There are different ways in which personal data can be modified to conceal identities:

Coded information contains information which could readily identify people, but their identity is concealed by coding. The key to which is held by members of the research team using the information.

Anonymised data with links to personal information is anonymised to the research team that holds it, but contains coded information which could be used to identify people. The key to the code might be held by the custodians of a larger research database.

Unlinked anonymised data contains nothing that has reasonable potential to be used by anyone to identify individuals.

As a minimum *anonymised data* must not contain any of the following, or codes for the following:

- Name, address, phone/fax. Number, e-mail address, full postcode.
- Any identifying reference numbers.
- Photograph or names of relatives.
- The *age*, if a small sample size is taken; in this case there has to be compromised between scientific precision and the protection of the individual privacy.
- Rare disease or treatment, especially if an easily noticed illness is involved.
- Partial post-code, or partial address.
- Place of treatment.
- Rare occupation or place of work.
- Combinations of birth date, ethnicity, place of birth, and date of death.

Researcher and database developer should always consider – when designing studies, before passing information to others, and before publishing information- whether data contain combinations of such information that might lead to identification of individuals or very small groups. How much of this potentially identifying information can be safely included in data that is assumed to be unidentifiable can only be judged on a case by case basis taking into account the sample size, the ways in which results will be published and used (Medical Research Council, 2000).

Within HUMABIO we will follow the unlinked anonymised data policy, excluding users having rare diseases and any other identifiers, except type of impairment (as category only, not with medical detail), age, gender and nationality. Once anonymised, the data will not allow tracing back the participant in any way. Other databases of participants will not be maintained, neither centrally nor locally.

4.3 International and European instruments in the field of data protection

a) The oldest European instrument is the European Human Rights Convention (EHRC, 1950) The relationship between the Community Law and the Convention of Human Rights can be shortly summarised as following: The fundamental rights, including these of the European Convention, form an integral part of the general principles of community law. This is explicitly laid down in art. 6 par. 1 & 2 of the Treaty on European Union (Amsterdam version). Thus, EHRC will be utilised as source of law by the European Court of Justice. EHRC has in addition legal effect in the national law of the States Parties that entered the Convention. However, EHRC protects the individual against infringements of the fundamental rights undertaken by the State or other public bodies. In relations between individuals or private bodies and individuals the effect of EHRC is unclear (so called "Drittwirkung" in German). Therefore, for instance in case of private and family life, the European Court of Human Rights requires the existence of appropriate rules in the national legal order protecting the essential features of private and family life against infringements undertaken by private bodies.

Art. 8 of EHRC protects the right to privacy.

According to two court decisions of the European Court of Human Rights the protection of medical data falls within the scope of art. 8. Its disclosure is legitimate only for the protection of other overriding rights, such as the investigation and prosecution of serious crimes, the exercise of other rights of the applicant, etc. The protection of privacy may also override the right to freedom of expression laid down in art. 10 EHRC (1950), since latter is restricted if necessary for the protection of the rights of others (such as the right to privacy) or for the prevention of disclosure of information received in confidence (art. 10 par. 2). Assuming art. 10 ECHR applies to the activities of Internet service providers including content providers (i.e. provider of a medical database), they may be found liable in case of infringement of a patient right to privacy according to art. 10 par. 2 ECHR (1950).

b) The Council's of Europe Convention for the protection of individuals with regard to automatic processing of personal data is the first European instrument in this field. It laid down the basic principles of a lawful data processing addressing the threats from the invasion of information systems, such as the data aggregation, at that time. In this respect, it concerns the *automatic* data processing, although the Member Countries could extend its applicability to non-automatic data processing. Art. 6 states that medical data may not be processed

automatically unless domestic law provides appropriate safeguards. The Convention is of limited importance for EU countries after the enactment of the EC Directives on data protection.

c) The Charter of Fundamental Rights of the European Union (2001) is the most recent achievement of the European Union in the field of fundamental rights. Of course, this effort had to face different legal cultures and political constraints. Thus, the Charter constitutes the common denominator of the legal cultures of the Member States, the international conventions to which the Member States are member and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights. For reasons relating to the tasks and powers of the European Union the Charter is solely a "solemn proclamation" and is not legally binding. It has rather a declaratory function and could be the first step towards to legally binding regulations providing that the Union will choose for a closer political co-operation. The Charter of Fundamental Rights is addressed to the institutions and bodies of the Union and the Member States only when they are implementing Union Law (art. 51).

The scope of the protected rights shall not exceed the level of protection and the meaning of corresponding rights set out either in the Community Treaties or the Treaty on the European Union (e.g. the freedom of establishment) or the European Convention for the Protection of Human Rights (art. 52). This practically means that the meaning, scope and limitations relating, for instance, to the protection of private and family life according to the EHRC (art. 8) and the Charter of Fundamental Rights (art. 7) shall be identical.

Nevertheless, the Charter of Fundamental Rights in the course of the respective legal trend dedicates a separate article to the protection of personal data. Article 8 sets out the right to the protection of personal data of an individual and thus the protection of personal data has now an own legal basis apart from the right to respect for an individual's private life and the protection of the human dignity. Art. 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Finally, Art. 8 sets out the need for an independent authority which shall control the compliance with the data protection rules.

d) In 1999 the Council of Europe has adopted the Recommendation (99) 5 on the Guidelines for the protection of privacy in the information highways. These Guidelines may be incorporated in or annexed to codes of conduct of Internet service provider to obtain legal validity. The Recommendation is in line with the EC Data Protection Directives regarding the principles of the lawful data processing, the duties of the Internet service providers and the rights of the data subject. The Recommendation encompasses a series of detailed information what the users and service providers shall do to reduce the risks arising from the Internet. It is worth mentioned that the users are required to use digital signature and encryption techniques. On the other hand, the service providers are required to use certified privacy enhancing technologies, to ensure data confidentiality and integrity as well as logical and physical security of the network and the services provided over the network. The service providers shall also incorporate detailed privacy statements on the web-sites. Finally, the communication of sensitive data, for instance medical data, for marketing purposes requires the previous, informed and explicit consent of the data subject.

e) The OECD is actively participating in the issues regarding the data protection, the data protection on the Internet as well as the protection of consumer rights with regard to e-commerce. First, OECD issued Guidelines governing the protection of privacy stipulating the fundamental principles (OECD, 1980).

In 1998, OECD issued a Recommendation with regard to the implementation of the aforementioned Guidelines on global networks. The Recommendation addresses mainly commercial sites offering various goods and services, such as tourism, air travel ticket sales, finance etc. It is not legally binding unless the Internet service providers stipulate this explicitly. Although the Recommendation does not address healthcare applications, its provisions might apply as following:

The Recommendation imposes the obligation to the web-site provider to refer with a hyperlink to the national legislation on data protection and the national Data Protection Authority. Moreover, every Data Protection Authority should be present on the Internet through relevant, well-documented and interactive sites. The web-sites shall also maintain on-line private statements giving details on the kind of data collected, the purpose of, the use of the clickstream data and processing to which they are subject, as well as the opportunity to opt out. In case of on-line payments by cards they should configure their systems in such a way that they ask for the card details once, provided that they store this information in highly secure files on non-networked computers. Warning messages on the risks of the Internet shall be provided in case of processing of confidential data. For confidential data the highest degree of security shall be implemented. The implementation of privacy enhancing technologies is also required. Moreover, web-sites should formally state the acceptance of full responsibility for the security and confidentiality of the personal data collected and processed. With regard to data subjects rights the Recommendation highlights the right to access on-line the information collected and stored directly or indirectly, i.e. clickstreams or purchased profiles.

4.3.1 Data Protection Directive 95/46/EC

In 1995, the EC Directive on the protection of personal data has been adopted by the Council. The Directive is the first attempt on EC level to recognise the right to privacy and harmonise the national laws. Some main characteristics of the Directive are that it applies equally to public and private bodies, to both automatic and non-automatic data processing, and that the protection is restricted to natural persons (as opposed to legal entities). Moreover, the data must form a part of a filing system, which is defined as any structured set of personal data accessible according to specific criteria.

The Directive lays down following core principles / measures with regard to data processing:

- The fairness and lawfulness of data processing.
- The purpose limitation principle (data shall be processed only for pre-specified purposes and stored for no longer than this is necessary for the pre-specified purposes).
- The proportionality principle (data must be relevant and not excessive for the pre-specified purposes).
- The data quality (data must be accurate, kept up to date and where necessary erased or rectified).
- Transparency principle (data subject must have access to the data relating to him and the controller must provide the data subject with a series of information relating to the data processing).
- Voluntary participation of the data subject (data subject must give unambiguous and informed consent).
- Adequate security measures. (The data controller shall implement adequate technical and organisational measures to protect personal data from infringements related to data integrity, availability and confidentiality. The security measures shall comply with the state of the art and be appropriate to the nature of the data and the potential risks represented by the data processing. Moreover, the implementation costs is a key point).
- Data concerning the health of an individual are sensitive data and thus subject to specific rules allowing its processing. The Directive does not further specify the meaning of data concerning health.
- Where the processing is likely to present specific risks to the rights and freedoms of the data subject, for instance where sensitive data are processed for purposes other than the medical treatment, the processing is subject to prior checks by the national Data Protection Authorities.
- The implementation of specific and effective rules with regard to the liability of the person infringing the provisions of the Directive.
- The recognition of self-regulation instruments for the proper implementation of the purpose of the Directive in the various sectors. In this respect, codes of conduct of medical associations or chambers shall specify the general principles of the Directive tailored to the needs of each professional activity.

Art. 8 of the Directive on the processing of data related to health states that the processing of medical data shall be prohibited, unless,

- the data subject has given his explicit consent (art. 8 par. 2 (a)) or
- this is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent (art. 8 par. 2 (c)), or

- the processing is necessary for the establishment, exercise or defence of legal claims (art. 8 par. 2 (e))
- the processing is required for the purposes of preventive medicine, medical diagnosis, treatment or for the management of healthcare services and where the processing is carried out 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 (art. 8 par. 3).

Moreover, the Member States shall determine the conditions for the processing of identifiers of general application (art. 8 par. 7).

The Directive lays down a series of rights of the data subject, for instance the patient: These are:

- The right of access to his / her personal data.
- The right of erasure, blocking or rectification of the data which do not comply with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to him/her.
- The right to a judicial remedy for any breach of the above mentioned rights.

The first three aforementioned rights may be restricted if this is necessary for reasons relating to the protection of the data subject or the rights and freedoms of others or to prevent a criminal offence or for reasons relating to public security.

Eventually, the Working Party on the protection of individuals with regard to the processing of personal data established within art. 29 of the Directive shall be mentioned. Its aim is to assist the Commission on all aspects related to data protection, i.e. contribute to the uniform application of the national measures throughout the EC, advise on any proposed amendment of the Directive or additional or specific measures to safeguard the right to privacy. The Working Party has issued a series of documents, amongst them also regarding data protection issues raised by the use of ICT.

4.3.2 Directive 97/66/EC on Data Protection in the Telecommunications Sector

This Directive applies to data processed in connection with the provision of telecommunication services in public telecommunications networks, in particular via ISDN and public digital mobile networks, and is aiming to protect the privacy right of natural persons, as well as the legitimate interests of legal entities. Non-publicly available telecommunications services fall within the scope of the general data protection Directive 95/46/EC (Recital 11 Directive 97/66/EC).

The Directive imposes to the telecommunications network provider and the provider of a publicly available telecommunications services a duty to safeguard the privacy of the users. This means that the service provider - if necessary in conjunction with network provider - shall ensure the security of its services in a similar way as under the Directive 95/46/EC. Moreover, the Member States shall take all relevant legal measures to ensure the confidentiality of communications, i.e. to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications without the consent of the users except when legally authorised, for instance for reasons of public security, prevention, investigation, detection and prosecution of criminal offences.

The Directive stipulates the right to privacy with regard to traffic and billing data, itemised billing, the presentation and restriction of calling and connected line identification and the unsolicited commercial calls. For example, alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, such as the use of calling cards, or the deletion of a certain number of digits from the called numbers mentioned in itemised bills. Traffic and billing data must be erased or made anonymous after a period during which the bill may be lawfully challenged or payment may be pursued.

With regard to calling line identification, the calling and the called user must have the possibility via a simple means, free of charge to prevent the presentation of the calling line identification of incoming calls. In the medical context the right of the calling party to keep his/her anonymity should be stressed. In particular, help-lines for some groups of patients such as HIV patients have an interest in guaranteeing the anonymity of their callers.

In case of unsolicited calls for direct marketing the Member States are free to choose between the opt-in or opt-out alternative to protect the users of the services. The opt-in or opt-out alternative means whether such call is allowed on the imperative of prior consent of the user only or in respect to users who stated that they do not wish to receive such calls. The opt-in alternative is, however, prescribed where automated calling systems without human intervention or facsimile machines are used.

However, short time after the transposition of the Directive in the Member States, this shall be amended in order to keep pace with the speedy technological developments. In July 2000 the Commission submitted a proposal for a revised Directive.

It is true, that the wording of the current Directive caused a series of discussions and/or different interpretations whether the Directive is applicable to all kind of electronic communications. In fact, the Directive uses a terminology based on ISDN technology. Terms such as "calls" allude to traditional and ISDN telephony and make its applicability difficult to Internet services. European Commission's intention is now to ensure the protection of the right to privacy on the Internet.

The term "calls" is replaced by the term "electronic communications" and "electronic communications services". The notion "calls" will be further used only where the legislator envisages the telephone calls. The term "electronic communications services" is defined, in art. 2 b) of the proposed Directive establishing a common framework for electronic communication services and networks. Accordingly, electronic communications services include transmission and routing of signals on electronic communications networks. Thus, within the scope of the revised Directive would fall the Internet Service Providers, such as the Access Service Providers. - Content service providers do not fall within this scope -. By the replacement of the term "call" through the term "electronic communications" packet switched transmissions are covered without any doubt.

With regard to traffic data, the revised Directive extends the confidentiality of communications to traffic data. This has been regarded as a very positive measure, since on Internet it is difficult to separate in technical terms between content and traffic data. Login data, amount of data transferred, time and ending of session should be included within the scope of current Art. 6 Directive 97/66/EC. The revised Directive would in addition cover traffic data, such as protocol headers (TCP-header, IP-header etc.) which are read in every

router a packet passes through, header information (which might include content information). Traffic data shall be erased upon the termination of the call or in the revised Directive upon termination of the transmission (Data protection working party, 2000).

The revised Directive introduces the possibility of further processing for the provision of value-added services if the subscriber has given his/her consent. Value-added services, might be offered if location data are processed. Location data which allows the exact positioning of a user shall only be used with the consent of the subscriber. The subscribers shall also be provided with a simple means to temporarily deny processing of their location data in the same way as such means exist for calling line identification. The only exception to the principle of prior consent would be the use of location data by emergency services and for purposes of public and national security and criminal investigations.

Finally, unsolicited commercial communication by the use of e-mail would be permitted only upon prior consent of the subscriber (opt-in alternative).

In on-line networks, hence, both Directives should be taken into account. The general Directive 95/46/EC on the protection of personal data is the relevant text to define the obligations of the person who initiates the processing of content data. The Directive 97/66/EC, on the other hand, establishes the obligations of the providers of services pertaining to the transmission of messages or the provision of access services. For instance, in case of transmission of emails the controller should be the person from whom the message originates and not the person providing the transmission service. The latter will be responsible to safeguard the security of the network and he will be deemed the controller only in respect to the additional personal data processed for the rendering of the service.

4.3.3 Art. 29 - Data Protection Working Party: Working Document on Privacy on the Internet

The Data Protection Working Party has been established by art. 29 of Directive 95/46/EC and is the independent advisory body on data protection and privacy. Its tasks are laid down in art. 30 of Directive 95/46/EC and in art. 14 of Directive 97/66/EC. The opinions and recommendations of the Working Party are not legally binding, reflect, however, the current trends on European level and influence the decisions taken by the European Commission and the Committee established by art. 31 of Directive 95/46/EC.

This working document seeks to raise awareness and to promote the public debate on issues of on-line data protection. It therefore provides detailed information on technical aspects of how the Internet and the communications through the Internet are organised and what are the main privacy risks arising from the use of the Internet. In this context, it aims at the same time to provide an interpretation of the data protection Directives in that field. It follows a "holistic" approach by basing the analysis of privacy risks, the obligations and rights of the involved parties on both the general data protection Directive 95/46/EC and the privacy and telecommunications Directive 97/66/EC.

The risks to privacy arise from the activities of the various intermediaries. For instance, the use of routers, e.g. the telecommunications nodes in the Internet, which have the characteristic that the information may pass through a non-EU country which may or may not have adequate data protection, if this at the time of transmission is the "shortest" way of transmission.

According to the opinion of the Working Party, Directive 97/66/EC applies to telecommunication service providers who connect Internet users and ISPs and access service providers who provide the requested Internet service, transfer the request from the Internet user to proxy server and then to the requested website. It also applies to providers of routers and connecting lines. Moreover, the Directive 97/66/EC shall apply also to Internet Service Providers (ISPs) providing hosting services, such as portal services, who may log the requests, the referring pages and post cookies on the hard disk of the user and make profiles. The latter is, however, arguable since the host service providers transmit content information and thus it should rather come under the general data protection Directive. The working document recognises that the applicability of the Directive 97/66/EC to the activities of the host service providers is not always clear. When the provider hosts its own portal site comes under the general data protection directive whilst it comes under the specific when he plays the role of the access service provider.

The providers of Internet services, dependent on the aforementioned distinctions, are subject to the obligations to confidentiality and security laid down in both Directives (art. 4, 5 97/66/EC, art. 6 - 8, 16, 17 95/46/EC). Traffic data provided by providers of routers and connecting lines, ISPs and telecommunication providers shall be protected as content data according to art. 5 of Directive 97/66/EC as this is the case in the proposal for an amendment of 97/66/EC.

Interception of communication is unacceptable unless it fulfils three fundamental criteria in accordance with art. 8 (2) EHRC, and the European Court of Human Rights interpretation of this provision: a legal basis, the need for such a measure in a democratic society, and conformity with one of the legitimate aims listed in the Convention.

The Working party strongly recommends the use and offer of encryption tools by the providers of email services at no additional cost. The providers should also offer secure connection for the transmission of the emails. The need of integrity and authentication should be considered as well.

A means for ensuring encryption is the Secure Socket Layer (SSL) which is implemented in the most popular browsers and establishes a secure channel between the client and server computers. This is achieved by means of encryption and digital certificates. SSL enables the authentication of the server to whom the information shall be sent and the integrity of the data. It does not ensure the authentication of the client. These difficulties shall be overcome by the protocol SET (Secure Electronic Transactions) that provides for confidential transmissions using encryption, authentication of the parties, integrity and non-revocation (through digital signatures). The Working Party seems to support the use of the SET protocol instead of SSL, especially when sensitive information, such as the credit cards data, will be transmitted. Moreover, if a higher level of security is needed, the digital certificates should be stored on smart cards.

All the above EV Directives and International Agreements will be fully adopted within HUMABIO. The conformance to them will be safeguarded by the HUMABIO Ethics Committee.

4.4 Technical implementation in HUMABIO

Within the scope of HUMABIO data security privacy of communications will be accomplished through implementation of the Secure Sockets Layer protocol (SSLv3), which is known to be as safe as the underlying encryption algorithms (SSL itself does not imply the use of specific algorithms, but rather provides a secure frame for initial authentication and key exchange).

SSL is also widely spread and readily available on most operating systems. SSL requires two different algorithms, one symmetrical algorithm for the actual data encryption and another (asymmetrical algorithm) to exchange the single symmetrical encryption key used on both sides of the communication. Only a very limited number of asymmetrical encryption algorithms exist – nearly all of them sharing more or less the same strategies. RSA is the only commonly used algorithm – we recommend a key length of 1024 bits or higher, which is at present known to be impossible to hack in a reasonable amount of time (several millions of years using brute force on currently available equipment). A wider range of symmetrical algorithms is available, which differ in two relevant aspects: speed and strength. RC4 is considered a good balance, being simple, very fast and providing a similar strength to RSA/1024 using a key length of 128 bits.

Other algorithms may be taken into consideration, like IDEA or DES, both requiring somewhat more CPU time. SSL allows for negotiation of feasible algorithms at connection time.

SSL also requires at least a server-side authentication, allowing the client to be sure it is communicating with the expected host. An SSL-server may also request the client to authenticate itself through a signed X.509 certificate. This two-way authentication guarantees a perfectly safe communication between server and client, but may not – under all circumstances – be possible.

An alternative method is username/password authentication. After establishing a secure SSL communication between server and client, the client can send a username/password combination to the server. Since encryption is active, it is not possible for an intruder to read the contents of an authentication packet, though it is possible to implement a challenge authentication method as an additional measure, to allow the server to validate the client's identity (making sure the client knows the required password) without actually transmitting the password itself. EAP extensions

Paleker (2004) and Funk (2004) allow client and server mutual authentication, and also allow for confidentiality and integrity of the authentication information exchange.

4.5 HUMABIO privacy policy

Data taken within experiments or surveys contains private information (e.g. facts about relatives and relationships etc.). This information is sensitive and private for many people. Within HUMABIO, participants have to be asked an agreement (informed consent) before private information can be collected. Within this document it will also be stated, that the confidentiality will be preserved.

- It will be prevented to reveal the identity of the participants in research deliberately or inadvertently, without the expressed permission of the participants.
- The data will only be disseminated among partners after anonymisation.
- Information about the identity of the participants will not be stored after data has been collected.

- Confidentiality of data will be guaranteed in removing the confidential information or in restricting the access in some way.

As a minimum anonymised data will not contain any of the following: Name, address, phone/fax, number, e-mail address, full postcode, photograph or names of relatives.

Professional requirements have been adopted by law and obtained mandatory character based on legal sanctions. Medical secrecy rules seek to protect the disclosure of patient information to third parties, other than the medical practitioner in charge and the personnel working on his behalf. The medical practitioner may only by exception disclose such information. The rules may thus be interpreted as a right of the patient in addition to the obligations of the medical practitioner and his personnel. Medical secrecy rules and rules relating to the use of ICT may be also found in self-regulation texts, i.e. codes of conduct drawn by the Medical Associations or Chambers.

The automatic data processing made it necessary to extend existing schemes of secrecy and / or privacy in order to protect individuals from unauthorised and unfair automatic processing of their personal data.

The scope of data protection legislation is broader. The threats of automatic data processing required a complete regulatory framework to ensure -apart from the disclosure- the lawful collection, storage, modification, deletion and communication of the electronic data. Data protection legislation addresses, moreover, not only the need for data confidentiality, but the need for data quality including thus -apart from the confidentiality- the need for data integrity and availability as well as the need to trace the data processing. A further characteristic of data protection legislation is that it assigns roles and obligations; for each role, such as with regard to the data processor and the data controller, taking into account the necessary work-sharing for the maintenance of information systems. Moreover, data protection legislation recognises different categories of personal data, i.e. sensitive and non-sensitive data. Personal information or information related to health of an individual is considered as sensitive.

In the earlier 1970s the first Data Protection Act in Europe came into force. After this, other national jurisdictions followed, and international statutes came into force. Finally, the EC Data Protection Directives in 1995 and 1997 created the Community framework for the data protection.

In the chapter above, we presented current European and international instruments in the field of data protection.

5 HUMABIO Identity management

In this section technical solutions to the security issues in the above mentioned chapters will be envisaged. One important issue regarding data protection is Identity management. Workpackage 5 is dealing with this issues and as soon as an “**Identity management and biometric information interchange**“ structure is clarified it will be included in this Manual. In general “Identity Interoperability Services” need to ensure uniform levels of personal data protection, including measures in which individuals have the right to choose whether their data may be used for purposes other than those for which they originally supplied the data in question. Appropriate information regarding the data processing activities should be made available to the concerned individuals. Full compliance with the existing European and national data protection legislation should be ensured. In particular, work on interoperability should be co-ordinated with the mechanisms already in place following the Directive 95/46/EC16 (in particular article 29). When available, technologies that are privacy-compliant and privacy-enhancing should be used. Within the development of an authentication concept for the interoperability of the HUMABIO database it is foreseen that clients will need password, e.g. with an PKCS-7 Certificate (<http://www.networksorcery.com/enp/data/pkcs.htm>) using a bi-directional authenticated SSL- connection (T5.2).

6 Risk assessment

The following list offers the eight guiding principles of eHealth code of ethics (Internet eHealth Coalition, 2000 in Anderson & Goodman, 2002). The different topics show a huge overlap with some of the aforementioned principles.

- Candor:
 - disclose vested financial interest
 - disclose key information for consumer decision
- Honesty:
 - present information truthfully
 - No misleading claims
- Quality
 - accurate, clear, current, evidence-based
 - readable, culturally competent accessible
 - citations, links, editorial board policies
- Informed Consent
 - privacy policy and risks
 - data collection and sharing
 - consequences of refusal to consent
- Privacy
 - prevent unauthorized access or personal identification of aggregate data
 - let users review and update personal data
- Professionalism
 - abide by professional codes of ethics
 - disclose potential conflicts of interest
 - obey applicable laws and regulations
 - point out limits of online practice
- Responsible partnering and links
 - choose trustworthy partners, affiliates

- maintain editorial independence from sponsors
 - tell users when they are leaving the site
 - provide management contact info
 - encourage user feedback
 - respond promptly and fairly to complaint
- Accountability

In the HUMABIO project are no direct risks to the participant like in medical testing. The risks are more indirect. In general it is almost impossible to conceive a procedure, investigation, or process which would be without any risk. The importance of risk from the prospective of the participant should be considered as most important. In the process of “Informed Consent” risk and benefit should be outlined to the participant. Also his/her life situation/personality may substantially influence the way in which a risk is perceived. The end point of the process consent will be given by the person to be part of the research project having considered all aspects of the process and asked all relevant questions. All relevant information – is given to the participants. This means that the project *HUMABIO* will be *carefully explained*, as described in the informed consent chapters. The choice that is made and the consent that is given will be without coercion or undue pressure being applied.

There will be possibilities to ask questions, detailed information also under Chapter Informed consent.

Categories of risk:

- There will be no risk to human welfare
- No physical damage within the experiments will be taken in HUMABIO. Any equipment connected to a participant will be evaluated for personal safety (Before testing the newly developed sensors will be validated in consideration of Biocompatibility, Electromagnetic Compability, with standard tests regarding ISO criteria). These tests will be performed for the complete configuration and not only for the individual equipment.
- Psychological consequences are carefully examined.
- Social inconveniences will be minimised (no additional stress for families, cost reimbursement for additional transportation costs, ...).

6.1 “Conflict of interest”

Regarding to the DoW page 97 any “conflict of interest” will be documented in the ethical manual. We consider this as a continuing process if any conflicts arise during the whole duration of HUMABIO:

“Many of our interactions are predicated on an asymmetry in the information possessed by the parties involved.”(Joseph and Cook, 2005). Regarding this quote in the context of HUMABIO it reflects one of the risk of the in “monitoring” and “validation” concepts. The accusation of the “vitreous worker” is not out of all reason. “Privacy” has to be respected as a major concern of the Ethical Advisory board to safeguard this issue.

7 Therapeutic and non-therapeutic research

The term therapeutic research is used to cover research on the treatment of the disease but also on its prevention (e.g. vaccination) and on diagnostic procedures.

The primary intention of all medical research is to acquire knowledge that will be of benefit to humanity as a whole – to all who are or may become ill. It can be distinguished between therapeutic and non therapeutic research. Therapeutic research is directly concerned with treatment and thus offers the possibility of immediate benefit for participants. Direct benefit for participants in non-therapeutic research is either unlikely or long delayed.

It may initially be difficult to make a clear distinction between innovative therapeutic procedures and research. Nevertheless, at some stage such procedures must be subjected to disciplined investigation.

It is a project that focuses on tangible results, but not on direct health effects; so the research of *HUMABIO* can be considered as *non-therapeutic research*.

8 Deception and Debriefing

8.1 Deception

Researchers do not conduct a study involving deception unless that they have determined that the use of deceptive techniques is justified by the study's significant prospective scientific, educational, or applied value and that effective non-deceptive alternative procedures are not feasible.

Researchers do not deceive prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress. Within HUMABIO it has to be more specified in WP 2 which "extreme emotional states" (page 53 DoW) are trying to be measured in Pilot 2 (office/laboratory emotional staging). Of course "panic" (page 66 DoW) will definitely not be induced by the investigator.

Researchers explain any deception that is an integral feature of the design and conduct of an experiment to participants as early as feasible, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection, and permit participants to withdraw their data (American Psychological Association, 2002).

No deception will take place within HUMABIO pilots. Of course it is doubtful if a person who is tired is fully aware that he/she is being monitored. But this is of negligible importance to the user and all gathered data will be communicated to him/her after the end of the test.

8.2 Debriefing

Sufficient information about the nature, results and conclusions of the research should be provided to the participant. Researchers are obliged to take reasonable steps to correct any misconceptions that participants may have (American Psychological Association, 2002).

Researchers also inform the participants about symptoms or diagnoses of diseases that have been discovered during the observation; especially if the symptoms have not discovered yet by a physician. Relevant test results will be provided to participants by a General Practitioner.

If tests point strongly to a participants incapability to drive a car, the participants will be informed hereof and advised to undergo further testing and examination by a medical / psychological traffic expert of her choosing.

The debriefing has to be documented and will be signed by both sides. Summaries and copies of research reports will be given to research participants in appropriate accessible formats (e.g. *.pdf, html, printed, in Braille oral communication, etc.).

Still, as HUMABIO does not perform either medical research or user assessment, the need for debriefing is expected to be minimal.

9 Organization and insurance issues

All partners are obliged to respect the user's privacy, informed consent as well as the safety requirements. They should be aware of risks involved while conducting the studies. The consequences of risks are to be borne by the partner individually and not to be shared with the project or other partners. Appropriate insurance or indemnity to cover the participant in a trial should be provided according to the regulations of the Local Ethics Research Committee (LREC). In any case the HUMABIO Ethics Advisory Board recommends insuring the participants.

9.1 Ethics control committee

Any organization performing experimental work with human beings or animals must have an ethics control committee that must evaluate all the aspects mentioned here and formally approve the experimental procedures.

9.2 Accessibility of Facilities and Services

In some member states it is unlawful to discriminate against disabled people by refusing them access to services or providing a lower standard of service. There are also laws that require service providers to make reasonable adjustments to the way they provide their goods, facilities and services to make them accessible to disabled people. In this respect, it is the responsibility of each partner of HUMABIO consortium to ensure that contractors follow these steps for the disabled people involved in the HUMABIO research:

- In organising any workshop, presentation or focus group, people who are invited are asked if they require special facilities, for example, signers and/or amplification.
- Buildings and rooms must be accessible for wheelchair users.
- Use of small typefaces should be avoided. In printed material, 14-point type is preferable (e.g. copies of handouts); on screen presentations should be clearly legible.

9.3 Reimbursement Schemes

DoW page 96: There will be no payment of participants for taking part in the research. Although stated clearly in the DoW the structure of the pilot plans might change and guidelines for incentives might be needed. The following paragraphs are written for this case.

9.3.1 Incentives for participants

Payment of incentives to research respondents should be considered in return for participation. Participants should not normally be paid for participation in standard cross-sectional experimental test, primarily because of large sample sizes and the large cost involved. There is also a danger of creating an 'incentives culture' if payment is expected for participation in all research, although the HUMABIO partners are aware of the increasing difficulties in recruiting participants.

However, incentives should be considered where the research is particularly onerous, for example, a very long survey interview (beyond the average 45-60 minutes), for most qualitative research (face-to-face interviews, diary completion or group interviews where

attendance is crucial and timing inflexible for the individual), or an ongoing commitment to a survey series.

Incentives should not normally be paid to respondents who are being tested in their professional capacity. Instead, they may need to be recruited through their employer and the involved HUMABIO partners should normally seek to gain their executive's permission to conduct the research during working hours. There may, however, be instances where it is appropriate to pay incentives to certain research groups. In the case where payment of incentives is being considered, it is suggested to introduce an Invitation To Tender (ITT). In this way, the HUMABIO partners would invite tenderers to discuss incentives and make proposals; and tenders should be asked to show incentive costs separately to the overall participation costs.

9.3.2 Legal basis for reimbursements as incentives

Generally, legal basis for paying incentives to benefit recipients without affecting benefit payments may be interpreted as such:

Small one-off payments (say 20-30 €) to benefit claimants can be paid because they should be treated as capital rather than income. However, larger sums of money constitute remunerative work, so it could affect all types of customers' benefit and better be avoided. But in any case, different practices may be applied in different Member States, and this should be examined.

Normally remunerative work would affect a customer's entitlement to benefit if they worked above a threshold (16-20) hours a week: if they worked less hours than the threshold per week, it may affect the amount of benefit they receive if they earned more than their earnings (it is possible, in some cases and in some member states, participants are allowed to earn the reimbursement amount of their participation in the HUMABIO research, without these earnings to being taken into account in the calculation of their benefit). In these cases, the involved HUMABIO partner should assess whether participation affects ability to work and whether participation in a given research affects their normal benefit provided by the state in order to be taken into consideration and to be avoided.

Therefore, in the cases where reimbursement incentive is foreseen, claimants should be made aware of the status of the payment in opt-out letters using the following terminology: 'If you do take part in the face-to-face discussion, you will receive XX € in cash, as a 'thank-you' gift for your help with this study. This will not affect your entitlements to benefit in any way.'

If an involved HUMABIO partner is ever in any doubt about a legal issue, he/she should refer it to its legal services and inform the HUMABIO Ethical Advisory Board.

9.3.3 The amount to pay

Legal ethical advice suggests clearly that payments should be small and a one-off. The HUMABIO partners involved should pay the same amount of money to each of its respondents. Previous practice suggests that, where it is appropriate to pay respondents incentives, new contracts could be established that pay roughly 15€ for a survey interview, 20€ to participants for in-depth face-to-face interviews, 25€ for focus groups and 50€ for a day long 'workshop'. However, this preliminary guidance will need to be reviewed by the involved HUMABIO partners.

9.3.4 Type of payment

Respondents can be paid in cash or with a gift voucher. The advantages of vouchers are that on the one hand they may be more suitable for vulnerable groups, such as 'chaotic' drug users or alcohol abuser (although this is not the case in HUMABIO), and on the other hand interviewers may feel more comfortable carrying them. It is also good practice when conducting research with children to use vouchers for incentive payments.

The advantages of cash are that it does not compromise the HUMABIO partner's neutrality if particular organisations' vouchers are given and also cash may be more useful to benefit recipients. Respondents should be paid after the interview/ study and a record of the payment received kept by the interviewer. HUMABIO partners involved are expected to use their discretion to decide the most appropriate method of payment.

10 Future steps

The template on ethical and legal issues has been developed and circulated to all partners, so as to collect practices and legislation in the various countries regarding the issues above. It is included in the Annex I 'Template on ethical and legal issues'. The objectives are to collect the nationally or organisationally adapted ethical issues mentioned in this manual, as per local usages of LREC (Local Research Ethics Committee).

All the issues mentioned in this manual are picked out as a central theme in the questionnaire on ethical and legal issues. The purpose is to collect information from the HUMABIO partners who are planning to conduct pilots, but it has also an educative function: to point the partners the relevant ethical issues that are described in this ethics manual.

Yet it is too early to summarise the results that will be gathered with the above mentioned document (questionnaire on ethical and legal issues). In the first ethical controlling report (month 16), a relevant summary will be given.

11 HUMABIO Ethics Advisory Board

All used assessment tools and protocols within HUMABIO Pilots will be verified beforehand by its **Ethics Advisory Board**, regarding their impact to users' well-being before being applied to the pilot sites. Three renowned experts in the field, chaired by an experienced ethics coach, constitute the project Ethics Advisory Board, assisted by further external experts, when needed. The Ethics Advisory Board assumes responsibility for implementing and managing the ethical and legal issues of all procedures in the project, ensuring that each of the partners provides the necessary participation in HUMABIO and its code of conduct towards the participants. All relevant liaisons with the Commission will be through the ethics coach.

The ethics advisory board was created (09. 03. 2006) with 5 members:

- **Prof. Dr. rer. nat. Jürgen Maes**, (*confirmed*)

University of the German Army Munich, Expert in Justice Psychology

- **Prof. Dr. V. Dittmann**, (*waiting for confirmation*)

Director of the institute for forensic medicine University Basel.

- **Dr. Alexander Bullinger**; (*confirmed*)

COAT-Basel, leader of relevant Ethics Advisory Boards in various other research projects, such as SENSATION, AWAKE, AGILE and ISLANDS

- **Prof. Helen Petrie, PhD** (expert) (*participation rejected*)

Prof. Helen Petrie has a long-standing interest in the ethics of research with human participants and has taught ethics to both psychology and computer science students.

- **Prof. Dr. Ullrich Meise** (external expert) (*confirmed*)

University Hospital Innsbruck, Prof. Dr. Ullrich Meise is an experienced Professor in Psychiatry at the University hospital of Innsbruck. Since many years he is also providing help to developmental regions in central Africa. Extra:

- **Prof. Dr. Thomas Penzel** (external expert) (*confirmed*)

Hospital of Philips-University, Marburg, Germany, Prof. Dr. Thomas Penzel is a very renowned and experienced sleep researcher at the University of Marburg, Germany.

Secretary Ethical Advisory Board:

COAT-Basel

Marcel Delahaye

Wilhelm-Klein-Str. 27

4025 Basel

Tel. +41 (0) 61 325 54 86

Fax. + 41 (0) 61 383 28 18

E-Mail: key@coat-basel.com

12 Recommendations

The Ethical issues under auspices of HUMABIO are listed within this manual. These are: Informed consent, Security issues, Privacy, Risk assessment, Identity management & the role of the ethics advisory board. The major ethical guidelines were examined and relevant information is summarized. Information about the partners is also being gathered throughout the questionnaire on ethical and legal issues.

The informed consent is a very important part of the research process; that is why a lot of space in the present manual is dedicated to this issue. The relevant facings of a valid informed consent for HUMABIO are described. No experiments are being performed with person unable to give a valid consent. The HUMABIO user groups do not include mentally disabled people.

Very important is that private information is held confidential. The chapter about risk assessment, points out the importance of the participant's view of the risk and finally results in his/her informed consent statement.

In short terms the HUMABIO research does involve experiments with human beings as described in this manual. No human biological samples will be taken. The personal data will be strictly protected and unlinked anonymised. No genetic information will be collected. No user personal data and preferences will be sent around in the Network, nor will be available to any third party (i.e. for advertisement, marketing or even research – outside HUMABIO objectives).

The goal of this manual was to compose a guide for all the researchers within HUMABIO. The major recommendations are:

- Possible threats or dangers to the participants need to be approved via a risk/benefit analysis and documented in the Informed Consent form.
- Benefits from advances in physiology and medicine, technology, security and work related safety derived throughout research within HUMABIO, will be made available to the public, with due regard for the dignity and human rights of each individual and insofar as none of the aforementioned ethical issues are violated.
- In the same form the access right to the collected data and their usage needs to be acknowledged.
- The level of anonymisation needs to be as high as possible and the process of anonymisation needs to start at an early stage of data collection.
- Data storage needs to be outlined and has to follow international guidelines.
- Personal information should not be retained longer than 3 month after the end of the project.

13 References

- American Psychological Association (2002). Ethical Principles of Psychologists and Code of Conduct. *American Psychologist*, 57, 1060-1073.
- Anderson, J.G. & Goodman, K.W. (2002), Ethics and Information Technology, A case based approach to a health care system in transition. Springer, New York.
- Charter of fundamental rights of the European Union. (2000) Nice.
- Council of Europe (1997). Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo.
- Committee of Ministers Council of Europe (1990). Recommendation (No. R(90)3).
- Data protection Act UK: www.opsi.gov.uk/ACTS/acts1998/19980029.htm
- Data Protection Working Party (2000). Privacy on the Internet – An integrated EU approach to On-line Data Protection, 5063/00/EN Final.
- Directive 97/66/EC of the European parliament and the council (1997). Concerning the processing of personal data and protecting of privacy in the telecommunications sector.
- Directive 2001/20/EC (2001). On the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use.
- EU Directive 95/46/EC The data protection directive (1995).
- European human rights convention (1950)
- Ethics in EU projects, Ethical issues in EU research proposals – checklist, updated 08.11.2005
in:
http://europa.eu.int/comm/research/science-society/page_en.cfm?id=3205
- Freeman, L. & Peace, G. (2005) Information Ethics: Privacy and Intellectual Property. Information Science Publishing.
- Funk, P., Blake-Wilson, S., (2004) EAP Tunneled TLS Authentication Protocol Version 1, work in progress
- General Medical Council (GMC) www.gmc-uk.org/
- Joseph, L. & Cook, D. (2005) in: Information Ethics: Privacy and Intellectual Property. Information Science Publishing. (p. 200)

- Johnson, D. H. & Sabourin, M. H. (2001). Universally accessible databases in the advancement of knowledge from psychological research. *International Journal of psychology*, 36, 212-220.
- Knapp, S. & VandeCreek, L. (2003). A guide to the 2002 Revision of the American Psychological Association's Ethics Code. Professionell Resource Press, Sarasota Florida.
- Medical Research Council (1993). The ethical conduct of research on the mentally incapacitated, London.
- Medial Research Council (2000). Personal information in medical research. In: Manual for Research Ethics. S. Eckstein (eds.). 367-390, University Press, Cambridge.
- OECD (1980). Guidelines governing the protection of privacy and transborder flows of personal data.
- Royal College of Psychiatrists (2000). Guidelines for Researchers and research Ethics Committees on Psychiatric Research involving Human Participants, Gaskell, London.
- Patry, P. (2000). Experimente mit Menschen. Einführung in die Ethik der psychologischen Forschung. Hans Huber. Bern.
- Palekar, A., et al. (2004), Protected EAP Protocol (PEAP), work in progress.
- Social Research Association (2003). Ethical Guidelines.
- United Nations "GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES" in: http://www.datenschutz-berlin.de/recht/int/uno/gl_pbden.htm
- UNESCO declaration 1997: z. B. in: <http://www.ruhr-uni-bochum.de/zme/unesco-1197.htm>
- World Medical association (2004). Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Participants, Tokyo.
- USA Secretary of Health and Human Service: www.hhs.gov/

Annex I Template on ethical & Legal Issues

INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME



HUMABIO

Project full title: **Human Monitoring and Authentication using Biodynamic**

Indicators and Behavioural Analysis

Proposal/Contract no.: 026990

Template on ethical and legal issues			
Milestone 1 WP 1			
Work package No.	1	Workingtask Title T1.3	Legal & ethical issues and project policy
Authors		Dr. Alex Bullinger (COAT) Marcel Delahaye (COAT)	
Status		Draft	
File Name:		Template_ethical and legal issues_T1.3	
Project start date and duration		01 January 2006, 30 Months	

Template on ethical and legal issues

To be filled-in by all HUMABIO partners

Ethical control instruments

1. At which level of organization, ethical controls are audited?

- laboratory or workgroup
- division or department
- institution
- regional
- national

2. Is there an international or national legislation, which you must follow when performing tests with human subjects?

- Yes
- No

If Yes, please give details (reference number and short description of procedure):

.....
.....
.....
.....
.....
.....

3. Is there an ethics controlling body in your country?

- Yes
- No

If Yes, please give details about the procedure:

.....
.....
.....

4. Is there an ethics controlling committee within your organisation?

- Yes
- No

If Yes, please give details about the procedure:

.....
.....
.....

5. Is there an established ethical control procedure which you must follow before performing tests with human subjects?

- Yes No

If Yes, please give a brief description of it:

.....
.....
.....
.....
.....
.....

Privacy

6. Is there an established Data Protection Authority which you must follow before performing tests with human subjects and their personal data?

- Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

7. Do you follow written procedures to protect privacy?

- Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

8. Do you follow any official national or international guidelines on protecting privacy?

- Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....
.....

9. Do you clarify to the participants that all data collected in the activities they are participating is kept confidential and that their anonymity will be protected?

- Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....
.....

10. Do you identify persons and their professions who are authorized to have access to the data collected?

- Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....
.....

Safety

11. Will you provide information to the participants if you get aware of an illness

- Yes No

If Yes, please give a brief outline and provide references.

.....
.....
.....
.....
.....
.....

12. Is every experiment evaluated for any biological or other effects?

- Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

13. Do you have written procedures for maintaining hygiene within your own group or institution?

- Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

14. Do you have written procedures for safety of employees and volunteers within your own group or institution?

- Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

15. Do you have procedures, facilities and expertise to test or verify equipment for patient safety to protect against electrical or magnetic hazards?

- Yes No

If Yes, please give a brief outline of it:

.....

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

16. Do you have procedures, facilities and expertise to test the patient safety of prototypes you develop?

Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

Risk assessment

17. Do you have procedures and expertise to verify bio-compatibility of the data collection system you use?

Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

18. Is your organisation insured against risks as a result of breach of privacy, safety and bio-compatibility?

Yes No

If Yes, please give a brief outline of it:

.....

.....
.....
.....
.....
.....

If No, please explain the reasons briefly or what corrective actions you take?

.....
.....

19. For conducting results ethically and manage the risk, do you need to involve other organization (unit, division, department etc.) that also control and decide your research activity?

Yes No

If Yes, please give a brief outline of it:

.....
.....
.....
.....
.....

20. What kind of signals regarding the physiological biometric profile/anthropometric authentication system do you measure?

If Yes, please give a brief outline of it:

.....
.....
.....

21. If applicable, please describe the intended / desirable improvement / enhancement of your specific physiological biometric profile:

If Yes, please give a brief outline of it:

.....
.....
.....

22. If applicable, please specify the shortcomings of the profiling system (regarding possible risks), etc.:

If Yes, please give a brief outline of it:

.....
.....
.....

ANNEX II HUMABIO Informed consent form template

HUMABIO Informed consent form template**1. GENERAL INFORMATION**

this part will be pre-filled by the investigator for each study

The HUMABIO Ethics Advisory Board reviewed this pilot study from the standpoint of the protection of human research participants. The HUMABIO Ethics Advisory Board found the study to be in compliance with the relevant regulations.

1.1 This version of the consent document was prepared on:

1.2 This trial was approved by the HUMABIO Ethics Advisory Board on:

1.3 Names of the investigators responsible for this project:

2. INFORMATION ON THE RESEARCH STUDY

the following issues should be explained by the investigator for each study to the participant before beginning the trial.

2.1 Title of the study

2.2 What is the purpose of this research study?

You are asked to take part in a research study under the direction of _____ . Other professional persons who work with him/her may assist or act for them.

These investigators are undertaking a research study to determine whether _____ . We expect to find _____ , which could lead to better methods of diagnosis / treatment / monitoring.

2.3 Who can take part in this study?

2.4 Why should I consider joining this study as a research participant?

2.5 Do I have to become a participant in this study? If I joined the study, can I change my mind and drop out before it ends?

2.6 What exactly will be done to me, and what kinds of treatments or procedures will I receive, if I agree to be a research participant in this study?

2.7 What kinds of harm can I experience in this study, and what will the investigators do to reduce the chances of harm?

2.8 What will the investigators do to make sure that the information they will collect on me will not get in the wrong hands?

2.9 What kinds of benefit can I expect personally from taking part in this study?

2.10 What kinds of benefit to others can come out of this study?

2.11 What will the investigators do, if I get injured in the study?

2.12 Will I get paid for taking part in this study?

2.13 Will I or my health insurance company be charged for any of the costs of this study?

2.14 Once I start in this study as a participant, what do I do if I want to find out more about the study, or to complain about the way I get treated?

2.15 Who gets to keep this document, once I sign it?

2.16 Which others may view or use the data of this document, if any?

3. DOCUMENTATION OF CONSENT

3.1 Research participant's identity

this part will be filled in by the participant.

The original will be kept by the investigator; a copy will be given to the participant.

Research participant's identity and the identity and dated signatures of the participant affirming that consent was given

The information shown below identifying the participant should be entered in the designated spaces at the time of execution of the consent document.

Participant's Name: _____

Participant's Birth Date: _____

Participant's Reference Number: _____

3.2 Participant Consent Form

this part will be filled in by the participant.

The original will be kept by the investigator; a copy will be given to the participant.

Title of the study:

Place of the study:

	Please circle as necessary	
I was informed about the effect to be expected, about possible disadvantages and about possible risks verbally and in writing by the test leader of the study.	Yes	No
I was informed about the purpose of research, the expected duration and the procedures verbally and in writing by the test leader of the study.	Yes	No
I was informed about the benefits to me or to others which may reasonably be expected from the research.	Yes	No
I was informed about the explanations on confidentiality (and limits) of the data.	Yes	No
I was informed about the right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing.	Yes	No
I was informed about whom to contact for questions about the research and research participants rights.	Yes	No
I have read and understood the written information handed out for the study mentioned above. My questions in connection with the study have been answered satisfactorily. I can keep the written information and receive a copy of my written declaration of consent.	Yes	No
I had sufficient time to take my decision.	Yes	No

In case an incident arises contrary to expectation, an insurance consists for me in the legally specified scale. The insurance was constructed by for this study.	Yes	No
I have spoken to: Dr./Mr./Ms.		
I understand that I am free to withdraw from the study <ul style="list-style-type: none"> ◆ at any time ◆ without having to give a reason for withdrawing ◆ and without affecting my future medical care 	Yes	No
I agree to take part in the study.	Yes	No
The confidentiality of my personal data was assured to me. Personal data will be used anonymised at the publication of the studies results. I approve of the fact however under a strict compliance with the confidentiality that the responsible experts of the authorities and the ethics commission may take a look for examining and control purposes of my original data.	Yes	No
If aftereffects appear, I will contact Dr./Mr./Ms. WITH THE TEL. NO.		

Signed

Date.....

Name (in block letters).....

3.3 Investigators' confirming statement

This part will be filled in by the investigator.

The original will be given to the participant; a copy will be kept by the investigator.

I have given this research participant information on the study, which in my opinion is accurate and sufficient for the participant to understand fully the nature, risks and benefits of the study, and the rights of a research participant. There has been no coercion or undue influence. I have witnessed the signing of this document by the participant.

Investigator's Name: _____

Investigator's Signature: _____

Date: _____

3.4 Research participant's identity (participant unable to read the form; to be provided in a appropriate alternative media e.g. large print, audiotape, Braille)

this part will be filled in by the participant.

The original will be kept by the investigator; a copy will be given to the participant.

Research participant's identity and the identity and dated signatures of the participant affirming that consent was given

The information shown below identifying the participant should be entered in the designated spaces at the time of execution of the consent document.

Participant's Name: _____

Participant's Birth Date: _____

Participant's Reference Number: _____