USAID
ՀԱՅԱՍՏԱՆԻ ՍՈՑԻԱԼԱԿԱՆ
ԲԱՐԵՓՈԽՈՒՄՆԵՐԻ ԾՐԱԳԻՐ
ARMENIA SOCIAL TRANSITION PROGRAM
14 Սունդուկյան, Երևան 14 Sundukyan, Yerevan
Telephone: (3741) 27-31-75/6/9
E-mail: rvaughan@padco.am
PADCO Inc., in collaboration with Abt Associates, AIHA, Counterpart International, QED, AMEG

REPORT No 7

PROTECTING INDIVIDUAL PRIVACY IN GOVERNMENT INFORMATION SYSTEMS IN ARMENIA: ISSUES AND RECOMMENDATIONS

Prepared by

PADCO Armenia Social Transition Program

December 13, 2000

PLANNING AND DEVELOPMENT COLLABORATIVE INTERNATIONAL

Development Solutions for the 21st Century

PREFACE

The implementation of a Personal Identification Number (PIN) for Armenia is central for improving the capacity of the Government of Armenia to administer social insurance and social assistance programs.

In the "Strategy for establishing identification code system for the social security sector in the Republic of Armenia" adopted by the Ministry of Social Security" in December 1999, the GOA emphasizes the need for improved data for administering social protection programs. The Strategy states:

> "In any field of work information plays critical role for ensuring efficiency. The possession of comprehensive information allows government agencies to administer programs efficiently, forecast the needs for and the costs of programs accurately and make right decisions in complex situations. The social sector is no exception. A great deal of information is processed in this sector which serves the entire population of the Republic. Incomplete or inaccurate information impedes the efficient implementation of reforms and also contributes to the creation of environment where abuses remain undetected."

Under USAID/PADCO Armenia Social Transition program, PADCO is assisting the Government of Armenia to implement the PIN system. The PIN system and the computerization of administrative databases as well as proposed improvements in telecommunications systems and widening access to the Internet raise serious questions about how to protect the privacy of individual citizens.

In its strategy, the GOA recognizes the need for rules to protect privacy. The concept document states (italics added):

> "To introduce the system, a Law on Social Security Identified Code System for Civilians of the Republic of Armenia should be enacted. This law will define the legislative basis for the system, rights and responsibilities of the parties, and regulate relationships within sector. The law will also define the procedures for stating information, for assigning identification code number, will list of data about individuals subject to collection, *and will establish privacy rules*. Sanctions for infringing the law also will be defined. The law will set forth the mechanisms for permitting private and state organizations use the identification for personification of individuals."

As part of the process of beginning the implementation of PINs and of computerizing the administration of government social protection programs, the Government of Armenia has requested assistance in preparing a "Law on Information" that will protect individual rights to privacy. The proper protection of privacy for individuals is also a requirement of the European Union for its member states.

This paper describes the issues that should be addressed in any comprehensive law on privacy. It also makes recommendations on how to address these issues based on standards adopted by the European Union, the USA and other countries. The paper was prepared by Steven Schiffman, legal consultant to the AST Program.

CONTENTS

PREFACE **2**

CONTENTS **3**

1. INTRODUCTION **5**

1.1. THE IMPORTANCE OF PROTECTING PRIVACY 5
1.2. THE SITUATION IN ARMENIA 5
1.3. PRIVACY IS ACCEPTED GLOBALLY AS A BASIC RIGHT 6
1.3.1. Privacy is a Basic Human Right *6*
1.3.2. Privacy Matters to the Public – as Employees, Employers, Consumers, and Patients *6*
1.3.3. Protecting Privacy Makes Sense - and Good Business Sense *6*
1.4. THE BASIC PRINCIPLES FOR PROTECTING PRIVACY 7
1.4.1. The Public Should be Informed of Their Rights to Privacy *7*
1.4.2. Privacy Should be Protected Under a Consistent and Comprehensive Legal Framework. *7*
1.4.3. Privacy Should Be Protected Using the Best Information Technology Available *7*

2. THE OBJECTIVES OF POLICIES TO PROTECT PRIVACY **7**

2.1. INTRODUCTION 7

3. GENERAL PRIVACY PROTECTION **8**

3.1. CONDITIONS OF DISCLOSURE 8
3.2. GOVERNMENT AGENCIES SHOULD RECORDS OF THE CIRCUMSTANCES UNDER WHICH THEY HAVE DISCLOSED PERSONAL INFORMATION 8
3.3. EACH GOVERNMENT AGENCY SHOULD ALLOW INDIVIDUALS ACCESS TO THEIR INDIVIDUAL RECORDS MAINTAINED BY THAT AGENCY 8
3.4. REQUIREMENTS FOR GOA AGENCIES 9
3.5. THE PRIVACY LAW SHOULD REQUIRE GOA AGENCIES TO ISSUE RULES FOR IMPLEMENTING PROCEDURES 10
3.6. GIVING COURTS THE JURISDICTION OVER CASES OF THE VIOLATION OF PRIVACY 10
3.7. GOVERNMENT CONTRACTORS 10
3.8. MAILING LISTS 11

4. MEDICAL PRIVACY ISSUES **11**

4.1. INTRODUCTION 11
4.2. IMPLEMENTING A SYSTEM OF PRIVACY AND SECURITY FOR MEDICAL INFORMATION 11
4.2.1. Issue at stake *11*
4.2.2. How to Implement Systems to protect the privacy of Medical Records *12*
4.2.3. Proposed Legal Provisions to Implement Systems to Protect Medical Privacy *12*
4.3. ENFORCING COMPLIANCE WITH MEDICAL PRIVACY PROCEDURES 13

5. PROTECTING PRIVACY IN HEALTH INSURANCE AND GENETIC TESTING **14**

5.1. POTENTIAL PROBLEMS 14
5.2. IMPLEMENTING PROCEDURES TO PROTECT THE PRIVACY OF GENETIC INFORMATION 14

6. SPECIFIC PRIVACY ISSUES: MEDIA, INFORMATION SOCIETY & DATA PROTECTION **15**

6.1. PRINCIPLES OF INTERNET PRIVACY (STILL IN DRAFT RESEARCH STAGE) 15
6.2. PRINCIPLE OF LAWFULNESS AND FAIRNESS 15
6.3. PRINCIPLE OF ACCURACY 15
6.4. PRINCIPLE OF SPECIFYING PURPOSE FOR DATA BASES 15
6.5. PRINCIPLE OF ACCESS TO INTERESTED PERSONS 15
6.6. PRINCIPLE OF NON-DISCRIMINATION 16
6.7. PRINCIPLE OF SECURITY 16
6.8. SUPERVISION AND SANCTIONS 16
6.9. FIELD OF APPLICATION 16

6.10. ADDITIONAL PROVISIONS 16
6.11. EXCEPTIONS AND RESTRICTIONS 16

1. INTRODUCTION

1.1. THE IMPORTANCE OF PROTECTING PRIVACY

As the Government of Armenia implements its programs to create a personal identification number for Armenians and to computerize record keeping systems for participants in social protection programs, concerns are being raised about the protection of people's "right to privacy". Privacy is a basic human right – recognized by all modern societies. With the computerization of government databases and the transfer of data about individuals through e-mail and by computer modem, however, protecting privacy becomes increasingly difficult. With electronic databases, personal data can be copied and transferred with a click of a mouse.

But this threat to privacy is wider than simply the threat posed by Internet data transfer or the computerization of records in health care providers and local social services offices. An individual's right to privacy is potentially violated when medical records are shared with third parties without the written permission and/or authorization of the individual. They may be violated when personal details are provided to insurance companies, when an employer demands data about an individual's results of a medical examination, when financial records are shared with the local tax administration or with other governmental agencies without the individual's approval and prior knowledge.

The key concern is that of confidentiality: knowing that the individual, alone, has the exclusive right and authority to share personal and time-sensitive data with other entities – governmental or private. Citizens of the Republic of Armenia should be confident that information requested by government agencies and private entities administering social protection programs will remain private and confidential. They should also be confident that there will be laws and sanctions to protect the privacy of such information and that those who violate such laws and regulations will face criminal and administrative penalties.

At the same time, the Government has the right to use data for the purposes of the administration of government programs. This also involves the sharing of data among different agencies – according to principles established through the legal and regulatory framework. For example, families applying for programs of targeted assistance – those based on the incomes and other qualifying characteristics of the family – should expect that the government will be permitted to request other agencies for information to verify the provided on their application form. But those verification procedures must be carefully defined under the law and the family required to sign a legal waiver. In most countries, this waiver to the right of privacy for certain information is included in the application form for welfare benefits.

1.2. THE SITUATION IN ARMENIA

The Constitution of Armenia, under Article 20(2) bans illegal collection, storage, use or dissemination of information about private life of citizens.[1] But an examination of the laws in Armenia that include provisions to protect privacy shows that existing protections are vague, inconsistent, non-implemented, non-sanctionable and inefficient.[2] Such laws that have some elements of protection consistent with the preceding characteristics include:

1. Law on Advocacy[3]
2. Law on State Statistical Data[4]
3. Law of RA on Auditing[5]
4. Law on Banking Operations & Secrecy[6]

---

[1] The section states: "The gathering, maintenance, use, and dissemination of illegally obtained information about a person's private and family life are prohibited".

[2] In this context, privacy includes protection vis-à-vis confidentiality, trade secrets, data and information flow, fiduciary requirements, lawyer-client privilege, doctor-patient privilege, cleric-believer privilege, banking secrets, tax records, medical records, insurance coverage, pension data, etc. These are examined in terms of international and regional standards, e.g., WTO, UN conventions, EU conventions, European Convention on Human Rights, etc.

[3] Article 8

[4] Article 8

[5] Article 18

[6] Paragraph one deal with the supervision of banks and their customers; Article 4 provides that the commercial banks are considered as customers of the Central Bank. Article 6 of the law defines the publication of the bank secret, Article

5. Law of RA on Constitutional Court[7]
6. Law of the RA on the Judiciary[8]
7. Law of RA on the Status of Judges[9]
8. Law on Prevention of Maladies Occurring from AIDS[10]
9. Law of RA on Prosecutor's Office[11]

1.3. PRIVACY IS ACCEPTED GLOBALLY AS A BASIC RIGHT

The need to protect individual privacy has been accepted throughout the world for three reasons:

1. It is a basic human right;
2. People are concerned about the potential for the misuse of government databases; and
3. Appropriate protection of privacy makes good business sense.

1.3.1. Privacy is a Basic Human Right

In democratic countries, privacy is regarded as a basic human right, protected through international conventions, national constitutions, tradition and culture. National parliaments and international organizations like the Council of Europe and the OECD have developed legal safeguards for the protection of privacy in connection with the processing of personal data. In October 1995, the European Union adopted a Directive to harmonize national legislation in this field, and to provide "a level playing field" for all activities, which increasingly relate to or depend on the processing of personal information. The EU Directive and the corresponding laws adopted by member nations provide the legal framework within which responsible companies do business and deliver their services. This is relevant for business within the EU and for data flows to third countries, since the Directive also deals with the existence or non-existence of adequate levels of protection in those third countries. The United States of America passed its first privacy protection law in 1974.

1.3.2. Privacy Matters to the Public – as Employees, Employers, Consumers, and Patients

The Government maintains data about all citizens. How this data is collected, processed, and maintained affects the well being of everyone – at work and in their private lives. Recent research in Europe and in the US indicates that people do care about privacy and the protection of personal information maintained by governments.[12] The same research shows that this is particularly relevant for the development of electronic commerce and for the use of the Internet: how to secure "trust and confidence" of consumers is one of the key areas of attention, not only for privacy or data protection commissioners, but also for businesses specializing in e-commerce and related services. In other words: the great expectations of the *Information Society*, both in a social and in an economic sense, depend in part on the way in which these privacy issues are handled and solved.

1.3.3. Protecting Privacy Makes Sense - and Good Business Sense

That means to take it serious, to invest in it, to deal with it in a positive and pro-active way, to act as good corporate citizens, and to develop good ways of "privacy governance".

---

8 stipulate rules for preserving the confidentiality; and Articles 9 – 16 stipulate the procedure for granting or refusing to grant access to the confidential information.

[7] Article 20 states that access to information by the mass media may be restricted if the information deals with the security of social structure, public life, national policy, and private life. The restriction should be decided so by the Court with the majority voting principle.

[8] In Article 9 closed sessions are held only by the court decision, as provided to the procedures defined in the law, and concerning the issues which jeopardize social structure, public life, national security, protection of the parties' private life, and protection of justice.

[9] Article 14 (IV) states that a judge does not have the right to disclose secret information on consultation of judges and results of voting, as well as investigation data obtained during the closed court sessions, while being at service and after learning it.

[10] Article 14.

[11] Article 6 (II) provides that the prosecutor, as well as the investigation officer is not obliged to give information on the cases under their investigation, which may concern the parties to the case, or provide access otherwise than foreseen by the Law.

[12] See XXX

1.4. THE BASIC PRINCIPLES FOR PROTECTING PRIVACY

To be effective, privacy policy should contain at the minimum, the following four elements.

1.4.1. The Public Should be Informed of Their Rights to Privacy

It is important to inform the public and people involved in the administration and protection of privacy about why privacy is a concern and the rights of people to privacy. People also need to understand their own obligations to provide accurate information and how they can ensure that information maintained in public databases is accurate. This should be a continuous effort, not only for data protection authorities, but also for all social and governmental organizations.

1.4.2. Privacy Should be Protected Under a Consistent and Comprehensive Legal Framework.

The Government of Armenia should adopt a national law on data and information in line with both international norms and with regional conventions such as the EU directives on privacy as well as on data protection.

1.4.3. Privacy Should Be Protected Using the Best Information Technology Available

New information technologies (IT) adopted by the USA and the European Community allow the effective protection of privacy. Access to databases can be carefully guarded and monitored. Armenia can take advantage of the progress made in other countries to protect its new computerized databases and communications systems. Independent audits of database systems and other means of verification should be included to ensure the management of the quality of information included in databases in a system for quality management and quality control.

2. THE OBJECTIVES OF POLICIES TO PROTECT PRIVACY

2.1. INTRODUCTION

Broadly stated, the purpose of a law to protect privacy is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from governmental and private agencies' collection, maintenance, use, and disclosure of personal information about them. The law is to prevent or curbing illegal surveillance and investigation of individuals by GOA; and to prevent potential abuses presented by the GOA's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an individual's social security (or personal identification number—PIN) number.

The four major objectives of laws to protect privacy are:

1. To restrict disclosure of personally identifiable records maintained by agencies.
2. To give individuals increased rights of access to GOA government records maintained about them.
3. To give individuals the right to correct GOA government records maintained about them if they can show that the records are not accurate, relevant, timely, or complete.
4. To establish a code of "fair information management practices" that requires government agencies to comply with statutory norms for collection, maintenance, and dissemination of records in a structured, non-intrusive way.

In keeping with these policy objectives, new legislation to be introduced by the Government of Armenia should be aimed at achieving two goals:

1. Harmonize and consolidate existing and new protections within the legal framework of one Privacy law that will cover all aspects of information transfer: medical privacy, data privacy, internet privacy, Freedom of Information Access privacy, personal and financial details, social and family privacy, statistical privacy and most importantly, the right to see and correct existing misinformation or inaccurate personal information held by those bodies and agencies legally entitled to such personal information;
2. The need to ensure existing and new protections meet international and regional standards such as those of the World Trade Organization, the European Union, and United Nations conventions.

3. GENERAL PRIVACY PROTECTION

3.1. CONDITIONS OF DISCLOSURE

In general, unless there is written consent of the individual about whom the information pertains, an government agency or private firm maintaining a database should be prohibited from disclosing any such information to any person or another agency or private legal entity (database compilers).

In the case of GOA agencies, however, there should be exceptions to this general principle. For these agencies, disclosure of personal records would be allowed:

1. To those officers and employees of the agency which maintains the record who need the information for the performance of their duties;
2. To the GOA department (or equivalent) that is responsible for planning or carrying out a census or survey or related activity pursuant to the provisions of Armenian law;
3. To an organization recipient who has provided the government agency with advance adequate written assurance that the record will be used solely as for statistical research or reporting, and that the information is to be transferred in a form that is not individually identifiable;
4. As a record which has sufficient historical or other value to warrant its continued preservation by the GOA, or for evaluation by a GOA agency to determine whether the record has such value;
5. To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the Republic of Armenia for a civil or criminal law enforcement activity providing that this activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency that maintains the record specifying the particular portion of the personal information desired and the law enforcement activity for which the record is sought;
6. To an organization or individual who has described compelling circumstances that failure to disclose the information may directly affect the health or safety of an individual and when notification for the disclosure has been transmitted to the last known address of such individual;
7. To either the National Assembly of Armenia, or any committee or subcommittee thereof, upon presentation of a written request and notification to the individual;
8. Pursuant to the order of a court of competent jurisdiction.

3.2. GOVERNMENT AGENCIES SHOULD RECORDS OF THE CIRCUMSTANCES UNDER WHICH THEY HAVE DISCLOSED PERSONAL INFORMATION

In order to preserve public confidence in the protection of their rights to privacy, all governmental agencies should maintain accurate records, with respect to the records under their control, of the following:

1. The date, nature, and purpose of each disclosure of a record to any person or to another agency as well as the name and address of the person or agency to whom the disclosure is made;
2. Retain the accounting at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;
3. Make the accounting available to the individual named in the record at his request; and
4. Inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

3.3. EACH GOVERNMENT AGENCY SHOULD ALLOW INDIVIDUALS ACCESS TO THEIR INDIVIDUAL RECORDS MAINTAINED BY THAT AGENCY

Perhaps the most important element of a privacy law is an individual's access to his or her own files together with their absolute right to insist on:

1. full knowledge on what is being stated (or published) about them ;
2. the legal right to insist that their records be maintained accurately; and
3. the right to require a correction of their records (or, if the individual's claim is controversial, the individual's claims concerning alleged inaccuracies should be maintained as part of their records).

To comply with these individual rights, the law on privacy should specify procedures to ensure compliance by government agencies. Thus, each agency that maintains records should, upon request by any individual for access to his records, provide him with a copy of all or a part of the records in a form comprehensible to

the individual. The agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

Moreover, the agency should permit individuals to request and changes of their personal information if they can provide the agency with evidence demonstrating the errors in the agency's database. Agencies should be required to respond to such requests within a specified time period. For example, several countries require changes to be made in government databases within 10 working days from receipt of documented requests from individuals. Government agencies are often required to acknowledge in writing such requests; make any corrections requested by the individual, and/or inform the individual of its refusal to amend the record in accordance with his request, provide the reason for the refusal, and state how the individual may request a review of that refusal.

Any disclosure containing information about which the individual has filed a statement of disagreement before the disclosure should clearly specify what portion of the disclosed record is subject to dispute and provide – with the disclosed information – the statement by the individual disputing the data and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested. The agency should be exempt from these procedures if the disclosure of information is in made for the purpose of preparing a civil or criminal action in a court of law.

The privacy law should recognize circumstances in which confidential information should not be disclosed – even to the individual. The privacy law should not be applied to records maintained by a government agency involved in enforcing criminal laws (including the Ministry of Internal Affairs). This exemption should cover:

1. Information about criminal offenders (consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status)
2. Information compiled for criminal investigations, including reports of informants and investigators, and associated with an identifiable individual; or

To prevent the abuse of this exception, when the law on the protection of privacy is adopted, any agency wanting to claim this exception should be required to provide a written request to the GOA stating why its databases should be exempted from the application of the privacy protection law. In this way, the burden of exemption should be placed on the militia and the Ministry of Internal Affairs to show why they need certain information on a continuing basis and why this information should be kept secret from the people of Armenia.

3.4. REQUIREMENTS FOR GOA AGENCIES

One objective of the privacy law should be to ensure that government agencies maintain only that individual data that is needed for the efficient and effective administration of the programs administered by that agency. Information that individuals are asked to submit to government agencies should be non-intrusive in the affairs of Armenian citizens and residents. In this context, the privacy law should stipulate that government agencies and their local offices should:

1. Maintain in their databases information about individuals that is relevant and necessary to accomplish the legally-defined purposes of the programs administered by each agency;
2. Collect information directly from the subject individual;
3. Inform each individual supplying information about on:
   1) The specific legal authority which authorizes the collection and maintenance of the information and whether disclosure of such information is mandatory or voluntary;
   2) The principal purpose or purposes for which the information will be used;
   3) The consequences to the individual, if any, of not providing all or part of the requested information;
4. Maintain all records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual;
5. Prior to disclosing any information about individuals to any other person or agency make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;
6. Maintain no record describing how any individual exercises rights guaranteed by the Armenian Constitution unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to, and within the scope of, an authorized law enforcement activity;

7. Make reasonable efforts to inform individuals when any personal information is to be disclosed to other individuals or agencies as a matter of public record;
8. Establish rules of conduct for persons involved in the design, development, operation, or maintenance of government databases, and instruct such people with respect to these rules;
9. Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against threats to this security that could result in harm to any individual about whom information is maintained;

3.5. The Privacy Law Should Require GOA Agencies to Issue Rules for Implementing Procedures

The law on privacy, itself, should also stipulate how procedures to protect privacy will be enforced. Thus the law should require GOA agencies to issue rules that:

1. Establish procedures to inform individuals – if they ask in writing – about all records are maintained by the agency concerning the individual;
2. Define the time, locations, and procedures by which an individual can view the records maintained by the agency – including medical and psychological records – about the individual;
3. Establish procedures for reviewing requests from individuals to amend personal information (see above); and
4. Establish fees to be charged, if any, for providing copies of individuals' records.

3.6. Giving Courts the Jurisdiction Over Cases of the Violation of Privacy

The law will be enforced only if there are clearly established procedures and punishment for violations of the law. Therefore, the privacy law should specify that individuals may bring civil suit against the government agency whenever any agency or GOA agency has violated the law. Violations may include the failure of the agency to amend an individual's record as requested (and not providing a written explanation for this failure), or the failure to answer request within the specified time period, or the failure to maintain accurate, adequate, and timely records or of requests and of disclosures of personal information. The law should, therefore, specify that Courts of the Republic of Armenia have jurisdiction in the matters.

Moreover, the privacy law should contain instructions to the Courts to safeguard the interests of the people of Armenia. These instructions should include the following:

1. In any suit brought under this law, the court may order the agency to amend the individual's record in accordance with his request or in any way that the court may specify.
2. The court may assess against the Republic of Armenia reasonable attorney fees and other litigation costs reasonably incurred by individuals in cases in which the individual has successfully demonstrated that agency had violated the privacy law.
3. The court may require agencies to provide the individual bringing suit with any information improperly withheld from him.

Giving the courts jurisdiction over allegations of the violation of the law on privacy is only part of the process. There must be penalties imposed on individuals and agencies violating the privacy law. Penalties discourage the violation of the law. Thus, Armenia's law to protect privacy should specify that any employee of an agency, who has access to individually identifiable information and discloses that information through negligence or deliberately, can be subject to punishment – including fines, loss of employment, or even imprisonment.

3.7. Government Contractors

It is important to ensure that there are no loopholes in this privacy law – especially in terms of work being done by private contractors on behalf of the GOA. This issue will become increasingly important if private entities – including for-profit companies and non-governmental organizations – become involved in the delivery of social services. Consequently, the law should include provisions stipulating that any contractor, and employees of such contractors, should be considered an employee of an agency for purposes of privacy and disclosures. In other words, a private company under contract to an agency of the GOA would be subject to the same requirements of the law on privacy as government agencies. This would ensure that confidential information remains confidential and will not be abused by private entities and individuals that have access to government databases.

3.8. MAILING LISTS

Another potential loophole that should be filled under the proposed privacy law: an individual's name and address may not be sold, rented, or released by a GOA agency. For example the names of pensioners will not be sold to companies trying to do business with this particular social group. Another example would be a ban on the Ministry of Health from providing private entities with a list of the names of practicing physicians in Armenia, etc. Naturally, such a ban will include selling names of users who might access a particular GOA website on the Internet.

4. MEDICAL PRIVACY ISSUES

4.1. INTRODUCTION

Data about the medical history, past medical treatments, and medical diagnoses of people who have sought medical treatment from licensed health care providers presents special issues. On the one hand, a doctor may need access to a prospective patient (the unconscious victim of a traffic accident, for example. On the other hand, an individual may not want their personal history of medical problems disclosed to a potential employer, a health insurance company, or to family members. In the case of someone suffering from a communicable disease – AIDs, for example – an individual may not require information about their condition disclosed, but failure to do so may place other people at risk. An erosion of the right of privacy may reduce the willingness of patients to confide in physicians and other practitioners and may inhibit patients from seeking care. Health research and the prevention of the spread of disease often depends on access to both identifiable (and depersonalized patient health information.

The guiding principles for protecting the privacy of medical information are similar to those applied to other types of information, but the balancing of individual and public interest is often more difficult. The privacy law should recognize that there is a right to privacy with respect to health information, including genetic information, and that this right should be protected. The law should also facilitate the release and analysis of depersonalized health information to allow effective, accurate, and timely medical research. The law should require the Ministry of Health to create a "patient's bill of rights" which would ensure that people have access to health information of which they are the subject; and the opportunity to challenge the accuracy and completeness of such information by being able to file supplements to such information. In other words, an Office of Health Information Privacy, within the MOH would be required to:

1. Provide individuals with the right to limit the use and disclosure of protected health information;
2. Establish strong and effective mechanisms to protect against the unauthorized and inappropriate use of protected health information; and,
3. Establish strong and effective remedies for violations of these proposed regulations and laws.

The "Medical Privacy Bill of Rights" would guarantee:

1. Individuals have a right of privacy with respect to their protected health information and records.
2. An individual's privacy right means that the individual's consent is needed to disclose his or her protected health information and that the individual has a right of access to that health information.
3. The right of an individual to inspect, copy, and supplement the protected health information.
4. The right of an individual not to have employment or the receipt of services conditioned upon the execution by the individual of an authorization for disclosure.
5. The right of the individual to request segregation of protected health information, and to restrict the use of such information by employees, agents, and contractors.

4.2. IMPLEMENTING A SYSTEM OF PRIVACY AND SECURITY FOR MEDICAL INFORMATION

4.2.1. Issue at stake

The privacy law should ensure that patients' interactions with health care providers remain confidential while allowing health care providers to submit information to the agency – the State health Agency or a private insurance company – in order to be reimbursed for the costs of providing care. Because of the way in which health care is financed, many entities may need access to information about a patient. It is, therefore, impossible to prohibit the disclosure of patient information by health care providers to other agencies and entities. Once patient caseload information is maintained electronically, it is easy for individuals and even for businesses to use improperly. A national database on the medical histories of individuals allows personal

data to be shared with employers and insurance companies – as well as government agencies such as the State health Agency.

Confidence and trust between the doctor and the patient can only exist if confidentiality is assured. This assurance serves the public interest by encouraging patients to fully disclose information about symptoms and medical history to their health care providers. The erosion of the right of privacy reduces the willingness of patients to confide in physicians and other practitioners and inhibits patients from seeking care. But data is needed for research and to allow other health care providers consulted by the patient with quick and easy access to relevant data.

Therefore, the policy objectives that should shape the medical privacy law are:

1. To provide individuals with access to health information of which they are a subject;
2. To ensure personal privacy with respect to health-care-related information; and
3. To impose criminal and civil penalties for unauthorized use of protected health information thus ensuring strong enforcement of these rights.

Provisions in the law should recognize the use of electronic records (internet/intranet/LAN). Agencies and private companies in the health sector should be required to maintain accessible electronic records of each access, or attempt to access – authorized or unauthorized, successful or unsuccessful to protected health information. Data-processing systems should respect their fundamental rights and freedoms, notably the right to privacy, the well being of individuals which is recognized in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Therefore, the protection of individual privacy should apply equally to electronic as well as to "paper" records. The level of protection should not depend on the data techniques used.

4.2.2. How to Implement Systems to protect the privacy of Medical Records

To meet these objectives, the privacy law should require the creation of:

1. Uniform procedures to be used by state health agencies, employers, insurance companies, and medical providers when transmitting electronic health data is needed;
2. Regulations that directs insurance companies and GOA agencies to disclose only the minimum amount of patient information needed to accomplish a particular medical purpose;
3. Regulations that prohibit the release of medical information to private firms for marketing purposes;
4. Rules granting patients access to their own medical records and to request corrections to those records (as described in Section 3, above);
5. Rules that define how government agencies may receive access to medical records on the grounds of "public interest". But such access must be limited and granted through stringent review of requests.
6. Regulation that require state and private health insurance agencies, health care providers, and health insurance programs to notify patients of any disclosures of their medical information and to require patient authorization before certain types of disclosures;
7. Adequate criminal and civil penalties for violating privacy standards outlined in the regulations;
8. Strict guidelines that permit disclosure of health information without individual authorization to protect public health (in the case of detection of communicable diseases, for example), conducting medical research, improving the quality of care, and preventing fraud and abuse in health care financing systems;
9. Regulations that prevent employers from using health information in making decisions related to the hiring, firing, and promotion of employees; and
10. Mandatory procedures to ensure that all disclosures would be limited to the minimum necessary for the purpose of the disclosure.

4.2.3. Proposed Legal Provisions to Implement Systems to Protect Medical Privacy

To implement the procedures described above, the proposed law on privacy should include provisions to:

1. Recognize that people have a right to privacy of medical information – including genetic information, and that this right is protected under the law. The principles of protection should apply to any information concerning an identified or identifiable person.
2. Create incentives to allow "depersonalized medical information for purposes of public health research, where appropriate.

3. Designate an Office of Health Information Privacy within the Ministry of Health to protect that right of privacy. This department should use modern technologies to safeguard, to the maximum extent practicable, the identity of the subject of the protected health information in all work papers and all documents summarizing the health oversight activity. It should maintain only such information as is necessary to accomplish the purpose for which it was obtained. It should maintain such information securely and limit access to such information to those persons with a legitimate need for access to carry out the purpose for which the records were obtained. It should also remove or destroy any information that allows subjects of protected health information to be identified as soon as possible.
4. To guarantee to individuals access to health information of which they are the subject, and the opportunity to challenge the accuracy and completeness of such information, and the right to request segregation of protected health information, and to restrict the use of such information.
5. Provide individuals with the right to limit the use and disclosure of their health information.
6. Establish strong and effective mechanisms to protect against the unauthorized and inappropriate use of protected health information, with strong and effective remedies for violations, requiring the individual's consent is needed to disclose his or her protected health information.
7. Limit disclosure of protected health information to that information or portion of the medical record necessary to fulfill the immediate and specific purpose of the disclosure.
8. Require the Ministry of Health and private health providers to provide written notice of privacy practices required at the time an authorization is sought for disclosure of protected health information.
9. Specify circumstances under which medical information may be disclosed without authorization by individuals.
10. Specify that, with respect to protected health information created as a result of an individual's participation in an ongoing clinical trial, access to the information shall be provided consistent with the individual's agreement to participate in the clinical trial.
11. Require health care providers, health insurance programs, health oversight agencies, public health authorities, employers, health or life insurance companies, and education institutions to give written notice of the privacy practices with respect to the following:
    1) The procedures for an individual to authorize disclosures of protected health information, and to object to, modify, and revoke such authorizations.
    2) The rights of an individual to inspect, copy, and supplement the protected health information.
    3) The right of an individual not to have employment or the receipt of services conditioned upon the execution by the individual of an authorization for disclosure.
    4) A description of the categories or types of employees, by general category or by general job description, who have access to or use of protected health information within the person.
    5) A simple, concise description of any information systems used to store or transmits protected health information, including a description of any linkages made with other electronic systems or databases outside the person.

4.3. Enforcing Compliance with Medical Privacy Procedures

Compliance with the procedures and systems outlined above should be enforced. All health care providers, health insurance programs (state or private), health oversight agencies, public health authorities, employers, health researchers, law enforcement officials, and education institution should be required to establish and maintain appropriate administrative, organizational, technical, and physical safeguards and procedures to ensure the confidentiality, security, accuracy, and integrity of protected health information created, received, obtained, maintained, used, transmitted, or disposed of by such person. This would provide people with three benefits:

1. The policies and safeguards will ensure that protected health information is used or disclosed only when necessary;
2. The categories of personnel who will have access to protected health information are identified; and,
3. The feasibility of limiting access to protected health information is considered.

5. PROTECTING PRIVACY IN HEALTH INSURANCE AND GENETIC TESTING

5.1. POTENTIAL PROBLEMS

The medical part of the information privacy act should protect patients' privacy with respect to genetic testing. Without such protection, government and private entities may be tempted to exploit information. For example, employers may require genetic information as a condition for employment, pharmaceutical companies may use information in marketing new products. And private health insurance companies may use the information to deny coverage to "at-risk" individuals.

While health care providers and researchers in Armenia are only just beginning to engage in genetic testing, the privacy law should include necessary provisions today to prevent the emergence of legal loopholes as these practices become more widespread. The privacy law and implementing regulations should prohibit the disclosure of genetic test results without the consent of the person to whom the information pertain.

5.2. IMPLEMENTING PROCEDURES TO PROTECT THE PRIVACY OF GENETIC INFORMATION

Because of the special nature of genetic testing, the proposed privacy law should specify define terms and procedures to ensure that there is no legal misunderstanding either by the GOA, its agencies, the private sector or the courts. Perhaps the most important element will be to clarify the meaning of "Prior written consent" of patents seeking genetic testing. In order for a patient to give "prior written consent", the proposed law should require that the patient be given the following information prior to undergoing genetic testing:

1. A statement of the purpose of the test;
2. A statement that prior to signing the consent form, the consenting person discussed with the medical practitioner ordering the test the reliability of positive or negative test results and the level of certainty that a positive test result for that disease or condition serves as a predictor of such disease;
3. A statement that the consenting person was informed about the availability and importance of genetic counseling and provided with written information identifying a genetic counselor or medical geneticist from whom the consenting person might obtain such counseling;
4. A general description of each specific disease or condition tested for; and
5. The person or persons to whom the test results may be disclosed.

No government and/or private health care provider should test anyone for genetic information without first obtaining the prior written consent and should not be allowed to disclose the results of such tests to any person other than the subject thereof without first obtaining the informed written consent. Exceptions would only be allowed if the results disclosed will be used in confidential epidemiological or clinical research about genes, or learning about the genetic basis of disease, or for developing pharmaceutical and other treatments of disease. In addition, either the law or rules issued by implementing government agencies, should establish the following practices:

1. Insurance applicants (including GOA health insurance agencies) are not required to answer any questions concerning genetic testing.
2. No disclosure of such results of genetic tests without the consent of the person to whom the information pertains;
3. Forbidding the requirement of genetic tests results as a condition of employment or insurance;
4. Forbidding discrimination by insurance institutions based on the use of such results of genetic tests.
5. Forbidding managed care enrolment and fees discrimination based on genetic testing data.
6. Forbidding the issuing of health insurance based on unfair discrimination against persons because of the results of a genetic test or the provision of genetic information.
7. In our law, unfair discrimination means cancellation, refusing to issue or renew, charging any increased rate, restricting any length of coverage or in any way practicing discrimination against persons unless such action is taken pursuant to reliable information relating to the insured's mortality or morbidity, based on sound actuarial principles or actual or reasonably anticipated claim experience.
8. Forbidding discrimination for any employer, employment agency, labour organization, or licensing agency by:
   1) Refusing to hire or employ, represent, grant membership to, or license a person on the basis of that person's genetic information;

2) Collecting, soliciting or requiring disclosure of genetic information from any person as a condition of employment, or membership, or of obtaining a license;
3) Soliciting submission to, requiring, or administering a genetic test to any person as a condition of employment, membership, or obtaining a license;
4) Offering a person an inducement to undergo a genetic test or otherwise disclose genetic information;
5) Questioning a person about their genetic information or genetic information concerning their family members, or inquire about previous genetic testing,
6) Use the results of a genetic test or other genetic information to affect the terms, conditions, compensation or privileges of a person's employment, representation, membership, or the ability to obtain a license;
7) Terminating or refusing to renew a person's employment, representation, membership, or license on the basis of a genetic test or other genetic information; or otherwise, seek, receive, or maintain genetic information for non-medical purposes.

6. Specific Privacy Issues: Media, Information Society & Data Protection

6.1. Principles of Internet Privacy (Still in Draft Research Stage)

- Technological development makes it possible to contribute towards the respect of fundamental rights and freedoms, and in particular the right to privacy, when personal data concerning natural persons are processed;
- There is a need to develop techniques which permit the anonymity of data subjects and the confidentiality of the information exchanged on information highways while respecting the rights and freedoms of others and the values of a democratic society;
- Communications carried out with the aid of new information technologies should also respect the human rights and fundamental freedoms and, in particular, the right to privacy and to secrecy of correspondence, as guaranteed by Article 8 of the European Convention on Human Rights;
- Specific Privacy Issues: Information Access To Government Records.

6.2. Principle of Lawfulness and Fairness

Information about persons should not be collected or processed in unfair or unlawful ways.

6.3. Principle of Accuracy

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

6.4. Principle of Specifying Purpose for Data Bases

The purpose for a database and conditions for its use should be specified, based on appropriate laws and rules, and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

1. All the personal data collected and recorded remain relevant and adequate to the purposes so specified;
2. None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;
3. The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

6.5. Principle of Access to Interested Persons

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate

corrections or deletions made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees.

The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

6.6. Principle of Non-Discrimination

Data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

6.7. Principle of Security

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

6.8. Supervision and Sanctions

The law of every country shall designate the authority, which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of isolation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

6.9. Field of Application

The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

6.10. Additional Provisions

Personal data undergoing automatic processing shall be: obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

Any person shall be enabled:

1. To establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
2. To obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
3. To obtain, as necessary, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out;
4. To have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure if not complied with.

6.11. Exceptions and Restrictions

The only exceptions permitted are:

1. When such derogation constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
2. Protecting the data subject or the rights and freedoms of others.

Restrictions on the exercise of the rights may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

The GOA shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization trans-border flows of personal data going to the territory of another country.