

**PHASE II & III SUMMARY REPORT:  
HEALTH DATA PRIVACY AND CONFIDENTIALITY**

**IN RESPONSE TO**

**HOUSE JOINT MEMORIAL 20**

**A Joint Memorial Requesting the New Mexico Health Policy Commission to Review  
and Make Recommendations Regarding Health Data Privacy and Confidentiality  
and Health Data Security Standards**

**Report presented and approved  
September 7, 2000**

**NEW MEXICO HEALTH POLICY COMMISSION  
2055 Pacheco Street, Suite 200  
Santa Fe, New Mexico**

## TABLE OF CONTENTS

1. OVERVIEW .....	1
2. HJM 20 PURVIEW AND GUIDANCE.....	1
3. WORK CHARTER.....	2
4. GENERAL PRINCIPLES CONSENSUS/DISAGREEMENT.....	3
5. RECOMMENDATIONS .....	3
ATTACHMENT 1 HOUSE JOINT MEMORIAL (HJM) 20: HEALTH DATA PRIVACY AND CONFIDENTIALITY AND HEALTH DATA SECURITY STANDARDS .....	4
ATTACHMENT 2 HJM 20 TASK FORCE MEMBERS – PHASE II & III HEALTH DATA PRIVACY AND CONFIDENTIALITY .....	11
ATTACHMENT 3 HJM 20: HEALTH DATA PRIVACY AND CONFIDENTIALITY AND HEALTH DATA SECURITY STANDARDS PROJECT PLAN ( <i>working document 03/01/00</i> ).....	15
ATTACHMENT 4 ITEMS REVIEWED BY THE PHASE II TASK FORCE .....	18
ATTACHMENT 5 SUMMARY OF GENERAL PRINCIPLES .....	20
ATTACHMENT 6 SUMMARY OF THE DRAFT “HEALTH INFORMATION PRIVACY ACT” .....	26
ATTACHMENT 7 PROPOSED DRAFT LEGISLATION:HJM 20 .....	29

## **PHASE II & III SUMMARY REPORT: HEALTH DATA PRIVACY AND CONFIDENTIALITY**

### **1. OVERVIEW**

This report summarizes the results of meetings held March through July 2000 by the New Mexico Task Force on Health Data Privacy and Confidentiality. The Task Force was convened by the New Mexico Health Policy Commission (HPC) in response to House Joint Memorial (HJM) 20, included as Attachment 1, which requests the HPC to review and make recommendations regarding health data privacy and confidentiality and health data security standards.

The Phase II & III meetings, facilitated by Michael Donlan, were attended by HJM20 Task Force members including representatives from state government agencies responsible for health, health care services, and insurance; the private health care sector; and individuals with security, technical, and pertinent legal expertise. Rosters of active and appointed Task Force members, as well as other individuals, who attended meetings, are included in Attachment 2. Minutes of the Phase II & III meetings detailing the discussions that took place are posted under "What's New" on two web sites: [www.healthlinknm.org](http://www.healthlinknm.org) and <http://hpc.state.nm.us>.

### **2. HJM20 PURVIEW AND GUIDANCE**

HJM20 stipulates that the HPC, working with members of the health information alliance, will study and make recommendations in five areas:

1. The appropriate protection, access, use, disclosure, and electronic transmission security standards of personal health data.
2. Federal law and New Mexico law on health data confidentiality and privacy, electronic transmission of health data and security standards, and the health care industry and security technical standards.
3. The views of the New Mexico public and the balance between privacy and benefits to the state and health of New Mexico from access to personal health data.
4. The privacy rights of individuals, including the use and disclosure of personal identifiable health information and the need for authorization.
5. The technical capabilities of the health care industry and costs of security measures, especially in regard to implementation by small and rural health care providers.

Phase I of the HJM20 effort in 1999 consisted of background analysis, information gathering, and comparative review of federal proposals and New Mexico laws. The Phase I Summary Report was issued in March 2000 and is posted under “What’s New” on the two web sites mentioned above. Phase II of the effort, which began in March 2000, focused on federal and New Mexico law on electronic transmission security standards to ensure health data privacy and confidentiality. Phase III, which began in April 2000, consisted of developing a consensus of recommendations for legislation for New Mexico on health data privacy and confidentiality and electronic transmission security standards. The Project Plan is presented in Attachment 3 of the report.

Task Force efforts were guided by the following principles in HJM20 (1999):

- Individuals expect confidential, respectful treatment of personal information about their health.
- Many participants in the health care system and government have legitimate needs to access health care information in performing their roles and access to such information has potential benefits to the health of New Mexico and an effective, efficient health care system.
- Health data is increasingly collected, shared, analyzed, accessed and stored by a variety of entities.
- The Secretary of Health and Human Services, in accordance with Public Law 104-191, has made recommendations to Congress regarding confidentiality and privacy of health data and Congress is expected to establish a minimum level of protection, allowing states to impose requirements, standards, or implementation specifications that are more stringent. [Note: These recommendations are contained within *Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to Section 264 of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.*]

### **3. Work Charter**

At the first Phase II meeting on March 14, 2000, Dr. Kathy Ganz, HPC Director, explained that the Phase II Task Force was a continuation of a previous Phase I effort that focused on the privacy and confidentiality of health data. The task before the Phase II Task Force is to look at what security standards should be in place as health data is electronically exchanged. A listing of items reviewed by the Task Force is presented in Attachment 4. Dr. Ganz also stated that Phase III, will consist of developing a consensus of recommendations for legislation for New Mexico on health data privacy and confidentiality and electronic transmission security standards.

- ◆ Dr. Ganz announced that the HPC work plan has been approved by the Commission and that Pam Lambert from the UNM Institute of Public Law will be working on HJM20 Phase III draft legislation for the 2001 session. She asked the group to make

recommendations at the *concept policy level* that can be integrated into legislation for the State of New Mexico. The Task Force will make its recommendations to the HPC and then the HPC will present to the appropriate legislative interim committee a final assessment and recommendations concerning appropriate protection of health data by October 1, 2000.

#### **4. General Principles Consensus/Disagreement**

The general principles expressed by the HJM 20 Task Force in Phases II and III are listed in Attachment 5, designated by “area of consensus” (majority view) or “area of disagreement” (minority view) as understood by Task Force members. The list tracks the elements of the proposed Health Information Privacy Act, draft 7/31/2000. Note that some Task Force members who disagreed with the overall premise of legislation nonetheless may have agreed with a general principle.

#### **5. Recommendations**

The HJM 20 Task Force has met over a period from September 1999 – July 2000 to discuss the requirements of the memorial and to develop recommendations. During this process, the members have also been monitoring federal action on the issue. The Task Force worked with consideration of the fact that the federal Secretary of Health and Human Services issued proposed rules on the confidentiality and privacy of health data. Additionally the federal rule will set the minimum standard for individually identifiable data access, use and disclosure and an individual’s right to inspect, correct and restrict the release of their personal information.

The Task Force also worked under the premise that State law only supersedes the rule if the state’s law is more protective of an individual’s privacy. Through its work, discovery was made that New Mexico laws have some major gaps in terms of the many provisions in the federal rule. Once the federal rule is enacted, New Mexico will be subject to the federal rule, until New Mexico State statutes are revised. Therefore, the Task Force moved forward by developing recommendations in the form of proposed legislation. Attachment 6 presents a “Summary of the Draft Health Information Privacy Act” and Attachment 7 presents “Proposed Draft Legislation” in response to HJM 20 (1999).

# **ATTACHMENT 1**

## **HOUSE JOINT MEMORIAL (HJM) 20: HEALTH DATA PRIVACY AND CONFIDENTIALITY AND HEALTH DATA SECURITY STANDARDS**

## **ATTACHMENT 2**

### **HJM20 TASK FORCE MEMBERS— PHASE II & III: HEALTH DATA PRIVACY AND CONFIDENTIALITY**

## ATTACHMENT 2

### HJM20 TASK FORCE MEMBERS PHASE II & III: HEALTH DATA PRIVACY AND CONFIDENTIALITY

First Name	Last Name	Organization	Address	City	Postal Code	e-mail addr	FAX No.	Phone No.
		League of Women Voters		Albuquerque	87111			
Dale	Alverson	UNM Telemedicine Program	UNM 1005 Columbia, NE	Albuquerque	87131	dalverso@unm.edu	505-272-0800	505-272-8633
John	Aragon	AARP	804 N. 5th St.	Belen	87002			
Rumaldo	Armijo	Human Services Department	P.O. Box 2348	Santa Fe	87501	rumaldo.armijo@state.nm.us	505-827-7729	505-827-7703
Nancy	Bannister	UNM-Health Science & Svcs Bldg.	Room 305-G	Albuquerque	87131	nbannister@salud.unm.edu	505-272-6923	505-272-3338
Michael	Batte	Department of Insurance	P.O. Drawer 1269	Santa Fe	87504			
Marty	Berman	State of New Mexico	404 Montezuma	Santa Fe	87501	Marty.Berman@state.nm.us	505-476-0402	505-476-0401
Karen	Bootzin	Lovelace Medical Records	P.O. Box 27107	Albuquerque	87125			
Maureen	Boshier	NM Hospital and Health Systems Assn.	2121 Osuna NE	Albuquerque	87113	mboshier@nmhhsa.org	505-343-0100	505-343-0012
Matt	Braun	UNM Health Sciences		Albuquerque		mhbraun@salud.unm.edu	505-272-6923	505-272-3270
Paul	Brown	Department of Health	1190 St. Francis Dr. Runnels Bldg.	Santa Fe	87502	pbrown@health.state.nm.us	505-827-2530	505-827-0112
Randy	Chesley	UNM Health	1650 University	Albuquerque	87102	RChesley@salud.unm.edu		
Denise	Clegg	American Civil Liberties Union	P.O. Box 80915	Albuquerque	87198			
Alexandra	Corwin		507 W. San Mateo	Santa Fe	87505			
Ron	Darling	UNM Health Sciences, Epi & Cancer	2325 Camino de Salud, NE	Albuquerque	87131	ron@nmtr.unm.edu	505-272-8572	505-272-8580
Jerry	Dickinson	Department of Health	1190 St. Francis Dr., Runnels Building P.O. Box 26110	Santa Fe	87502	jdickinson@doh.state.nm.us	505-827-2930	505-827-0004
Rena	DiGregorio	NM Hospital and Health Systems Assn.	2121 Osuna NE	Albuquerque	87113	rdigregorio@nmhhsa.org	505-343-0012	505-346-0215

First Name	Last Name	Organization	Address	City	Postal Code	e-mail addr	FAX No.	Phone No.
Margo	Dittrich	NM Health Information Management Assn.	St. Vincent Hospital 455 St. Michael's Drive	Sant Fe	87505			
Mike	Donlan		300 Lomita Street	Santa Fe	87501			
R. Phillip	Eaton	UNM Health Sciences Ctr-Admin.	Health Science & Serv Bldg. 3rd Fl.	Albuquerque	87131			
Robin	Fowler	Human Services Dept.	Santa Fe	NM	87501	Robin.Fowler@state.nm.us	505-827-7729	505-827-7231
Kathy	Ganz	Health Policy Commissio	2055 South Pacheco, Suite 200	Santa Fe	87505	kaganz@hpc.state.nm.us	505-424-3222	505-324-3200
Kathy	Goodyear	Health Policy Commission	2055 South Pacheco, Suite 200	Santa Fe	87505	kfgoodyear@hpc.state.nm.us	505-424-3222	505-424-3200
Lynn	Harris	Information Technology	404 Montezuma	Santa Fe	87502	lynn.harris@state.nm.us	505-476-0401	505-476-0411
Jerry	Harrison	NM Health Resources	300 San Mateo, Suite 905	Albuquerque	87108	nmhealth@nmhr.org	505-260-1919	505-260-0993
Deborah	Hartz	Children, Youth and Families	1120 Paseo de Peralta	Santa Fe	87501			
Betty	Hileman	DOH/PHD/NM Vital Records and Health Statistics	1190 St. Francis Dr. Runnels Bldg	Santa Fe	87502	bhileman@health.state.nm.us	505-827-1751	505-827-2342
Kevin	Kellogg	NM Medical Review Association	P.O. Box 27449	Albuquerque	87125	nmpro.kkellogg@sdps.org	505-998-9899	505-998-9898
Fred	Hashimoto	UNM Health Science Center		Albuquerque	87131	fhasimoto@salud.unm.edu	272-9437	272-2147
Stuart	Hidalgo	NM Medical Review Association	P.O. Box 27449	Albuquerque	87125	nmpro.shidalgo@sdps.org	505-998-9899	505-998-9898
Ami	Jaeger	Biolaw Group, LLC	7 Ave. Vista Grande, Suite 7B-205	Santa Fe	87505	asje@bio-law.com	505-466-2818	505-466-4642
Robert	Johnson	NM Foundation for Open Government	P.O. Box 92197	Albuquerque	87122		505-345-7808	
Charles Anna Marie	Key Davidson	UNM-Dept. of Pathology	Cancer Res. Facility, Rm. G-01	Albuquerque	87131	amd@nmtr.unm.edu		505-272-3127
Louis	LaFrado	L&D Associates	5510 Amigo Way, NE	Albuquerque	87101	landd@att.net	505-856-2539	505-238-2422
Pam	Lambert	UNM/Institute of Public Law	School of Law	Albuquerque	87131	plams@unm.edu	505-277-7064	505-277-1052

First Name	Last Name	Organization	Address	City	Postal Code	e-mail addr	FAX No.	Phone No.
Linda	Lewis	LANL		Los Alamos		llewis@lanl.gov	665-3354	665-3891
Randy	Marshall	NM Medical Society	7770 Jefferson NE, Suite 400	Albuquerque	87109			
Marcia	Martinez	State of New Mexico, ITMO	404 Montezuma	Santa Fe	87501	Marcia.Martinez@state.nm.us	505-476-0400	505-476-0401
Barbara	Mathis	UNM Health Sciences Center	Room 305G	Albuquerque	87131	bmathis@salud.unm.edu	505-342-0595	505-272-9362
Joanne Bruce	Montgomery Lorenz	Qualmed/Cimarron Health Plan Cimarron	6100 Uptown, Suite 400 2129 Osuna Rd. NE	Albuquerque Albuquerque	87110 87113	blorenz@hchorizons.com	505-342-0595	505-342-4660
Regis	Pecos	Office of Indian Affairs	228 E. Palace Avenue	Santa Fe	87501			
Kym	Peters	DOH, Bureau of Vital Statistics	1190 St. Francis Dr. Runnels Bldg.	Santa Fe	87502	kpeters@health.state.nm.us	505-827-1751	505-827-0124
Ellen	Pinnes	Health Action NM	P.O. Box 8251	Santa Fe	87504		505-983-9637	505-983-9637
Jo	Powell	Health Policy Commission	2055 South Pacheco, Suite 200	Santa Fe	87505	yjpowell@hpc.state.nm.us	505-424-3222	505-424-3200
Richard	Quillin	Human Services Department	729 St. Michael's Dr. San Miguel Plaza	Santa Fe	87505	rquillin@state.nm.us	505-827-6286	505-827-7752
Pat	Rogers	Modrall Law Firm (for) NM Press Assoc.	Modrall Law Firm 500 4 <sup>th</sup> St. Albuquerque, NM 87104	Albuquerque	87103	pjr@modrall.com	848-1891	848-1849
Robert	Rubin	Lovelace Research Institute	P.O. Box 5890	Albuquerque	87185			
Zeke	Sedillo	Lovelace Health Systems	1400 San Mateo, Blvd.	Albuquerque	87108	zeke.sedillo@lovelace.com	505-268-2967	505-262-3838
R. Dale	Tinker	NM Pharmaceutical Association	4800 Zune, SE	Albuquerque	87108			
Olivia	Trujillo	Health Policy Commission	2055 South Pacheco, Suite 200	Santa Fe	87505	omtrujillo@hpc.state.nm.us	505-424-3222	505-424-3200
Rick	Ulibarri	Los Alamos National Laboratory	Information Technology Support, P.O. Box 1663, MSA103	Los Alamos	87532	eboy@lanl.gov	505-667-0365	505-665-0140
Catherine	Ullett	NM Press Association	2531 Wyoming NE	Albuquerque	87112	nmprss@earthlink.net	505-275-1449	505-275-1377
Michelle	Williams	UNM HSC Legal	HSC 8317	Albuquerque	87131	mfwilliams@Salud.unm.edu		272-4437

# **ATTACHMENT 3**

## **PROJECT PLAN: HJM20**

**(Working Document 03/01/00)**

## ATTACHMENT 3

### HJM 20: HEALTH DATA PRIVACY AND CONFIDENTIALITY AND HEALTH DATA SECURITY STANDARDS PROJECT PLAN

#### Background:

HJM 20 (1999) requests the HPC to develop recommendations to 1.) Ensure an appropriate balance between the privacy rights of individuals and the access, use, and disclosure of personal identifiable health data; 2.) Ensure protection of health data during electronic exchange of security standards for electronic transmission of personal identifiable health data, and 3.) Provide for New Mexico compliance with federal law.

The work for HJM 20 is divided into 3 phases:

- ◆ Phase I: consisted of background analysis, information gathering, and comparative review of federal proposals and New Mexico laws.
- ◆ Phase II: Task force efforts will focus on Federal and New Mexico law on electronic transmission security standards to ensure health data privacy and confidentiality.
- ◆ Phase III: consists of developing a consensus of recommendations for legislation for New Mexico on health data privacy and confidentiality and electronic transmission security standards.

The HPC will present to the appropriate legislative interim committee a final assessment and recommendations concerning appropriate protection of health data by October 1, 2000.

#### Work Completed to Date:

- ◆ A comparative legal analysis of existing privacy and confidentiality principles in New Mexico statutes and New Mexico statutes in terms of emerging federal policy was performed. Gaps and conflicts in New Mexico statutes were identified.
- ◆ Consensus was also developed on New Mexico's position on the Federal Health and Human Services proposed regulations through a facilitated task force. The white paper summarizing the Task Force's recommended changes to the proposed rule was

endorsed by the HPC on January 14, 2000. Comments on the proposed federal rule 45 CFR Parts 160-164 were submitted on behalf of New Mexico.

- ◆ The task force discussed principles, issues, and the rights of individuals regarding individually identifiable health information, as well as which identifiable uses and disclosures should be authorized or required. The task force developed a general consensus on the principles for proposed health data privacy and confidentiality in New Mexico.

#### Phase II:

Phase II includes:

- ◆ reviewing emerging technology, existing industry and proposed federal standards for secure electronic transmission of health data
- ◆ assessing industry technical capabilities and cost of security measures
- ◆ reviewing and discussing the appropriate protection of electronic transmission of personal health data
- ◆ developing a consensus for New Mexico standards for secure electronic transmission.

#### Phase III:

Phase III includes:

- ◆ developing discussion draft of proposed legislation based on consensus reached in Phases I and II
- ◆ reviewing, discussing and assuring that the five essential principles of which are boundaries, security, consumer control, accountability, and public interest are addressed in recommendations for proposed legislation
- ◆ developing consensus on recommendations for proposed legislation
- ◆ making recommendations to the HPC and then to the appropriate legislative interim committee and appropriate executive representatives.

#### Timelines:

Phase II: April 30

Phase III: June 30

Recommendations to HPC: July

Report to Legislative interim committee / Executive representatives: October 1

**ATTACHMENT 4**

**ITEMS REVIEWED BY THE HJM20**

**PHASE II TASK FORCE:**

**Security Standards for Electronic Transmission**

## **ATTACHMENT 4**

### **ITEMS REVIEWED BY THE HJM20 PHASE II TASK FORCE**

- Existing State Policies and Standards on Security and Internet
  - State of New Mexico Information Technology Management Office CIO IT Standards
  - State of New Mexico Information Technology Management Project Information Security Policies and Procedures
  - NMAC document
- Federal 1996 Health Insurance Portability and Accountability Act (HIPAA) Security and Electronic Transmission Standards
  - Department of Health and Human Services (HHS) 45 CFR Part 142, Health Insurance Reform: Standards for Electronic Transactions; National Standard Health Care Provider Identifier; Proposed Rules
  - Frequently Asked Questions (FAQs) About Security and Electronic Signature Standards
  - NPRM: Security and Electronic Signature Standards
  - HHS Administrative Simplification Rules

**ATTACHMENT 5**

**SUMMARY OF GENERAL PRINCIPLES**

**PHASE II & III TASK FORCE**

**ATTACHMENT 5**

**HJM 20 TASK FORCE**

**SUMMARY OF GENERAL PRINCIPLES**

The general principles expressed by the HJM 20 Task Force in Phases II and III are listed below, designated by “area of consensus” or “area of disagreement” as understood by Task Force members. The list tracks the elements of the proposed Health Information Privacy Act, draft 7/31/2000.

<b>HEALTH INFORMATION PRIVACY ACT, DRAFT 7/31/2000</b>		
<b>Section of Act</b>	<b>Area of Consensus</b>	<b>Area of Disagreement</b>
Overall Theme	Individuals have a privacy interest in their personal health information; the confidentiality of this information should be appropriately protected.	None.
Overall Goal	Legislation should be enacted to establish a uniform, systematic approach to the use and disclosure of, and individual rights of access to, personal health information; current protections are insufficient; harm from breach of privacy can be significant.	Need for legislation is not established; scope is too broad; implementation is too costly and burdensome; sufficient protections currently exist; requirements are difficult to understand; costs outweigh the benefits; other remedies are available for violation of privacy.
Sec. 3(D), (H): Definitions	“Health care” and “health care provider” should be broadly defined to encompass nontraditional practices and providers, because the privacy interests are the same as for traditional medicine.	Inclusion of nontraditional aspects of medicine is too far-reaching; the category of “health information custodian” with responsibility for safeguarding information and following procedural requirements is overly broad.

## HEALTH INFORMATION PRIVACY ACT, DRAFT 7/31/2000

<b>Section of Act</b>	<b>Area of Consensus</b>	<b>Area of Disagreement</b>
Sec. 4: General Provisions	Generally: Personal health information may be used for treatment, payment or health care operations, or as permitted or required by law, but otherwise its privacy should be protected.	None.
Sec. 4(H): General Provisions	Redisclosure of personal health information should be subject to similar protections as original use.	Difficult to regulate; could be too onerous depending on the recipient.
Sec. 4(I): General Provisions	Personal health information should remain protected for two years following an individual's death.	An individual's cause of death should be public information.
Sec. 4(J): General Provisions	Health information protections and rights of access should not apply to prisoners.	Prisoner health information should be afforded a limited degree of protection.
Sec. 4(K): General Provisions	Minors who legally consent to health care treatment should have authority to control disclosure of the resulting information.	Parents should be able to see the health information of their minor children.
Sec. 5: Disclosure History	Generally: Individuals should be able to find out who has seen or obtained their health information when this occurs outside of the expected realm of treatment, payment or health care operations.	Keeping a record of disclosures may be too burdensome on small providers.
Sec. 6: Disclosure Without Authorization	Generally: In some circumstances the public need for information, coupled with careful constraints on use, sufficiently outweighs individual privacy interests to allow disclosure without authorization.	None.

## HEALTH INFORMATION PRIVACY ACT, DRAFT 7/31/2000

Section of Act	Area of Consensus	Area of Disagreement
Sec. 6(E): Disclosure Without Authorization	Research needs may justify use of personal health information without authorization, if certain criteria are met and the information is protected.	Either individuals should always have an opportunity to consent/object to use of their information for research, or the criteria should be stricter.
Sec. 6(F): Disclosure Without Authorization	Personal health information may be disclosed based on a reasonable belief that it is necessary to prevent serious and imminent harm.	Standard for disclosure can be too easily manipulated to justify unwarranted disclosure.
Sec. 6(G): Disclosure Without Authorization	Personal health information may be disclosed to family members or close friends, if the individual has agreed or is unable to make a decision.	Individuals may not want their information disclosed to family or friends, yet be unable to object.
Sec. 6(H): Disclosure Without Authorization	An individual's presence in a health care facility and general condition may be disclosed, unless the individual has objected in advance.	This type of information should be publicly available, particularly when it is newsworthy.
Sec. 7: Disclosure With Authorization	Generally: Use and disclosure of personal health information for purposes outside of the realm of health care or the public policy exceptions should require individual authorization.	None.
Sec. 7(G): Disclosure With Authorization	Individuals may be charged a reasonable fee as reimbursement for the cost of retrieving and providing requested information (see also 8(E) and 9(E)).	Reasonable fee standard is too vague; should include a maximum allowable amount.

## HEALTH INFORMATION PRIVACY ACT, DRAFT 7/31/2000

<b>Section of Act</b>	<b>Area of Consensus</b>	<b>Area of Disagreement</b>
Sec. 8: Individual Access to Information	Generally: Individuals should have the right to see and copy their own health information.	None.
Sec. 8(A): Individual Access to Information	Requests for access to information should be responded to as promptly as required by the circumstances, within no later than 30 days (see also 9(A)).	Information should be made available sooner than 30 days, such as within 15 days.
Sec. 8(B), (D): Individual Access to Information	Requests for access to information may be denied if access reasonably could be expected to endanger life or physical safety; individual must be informed of right to independent review by another provider.	Individuals may not know how to find another provider to conduct an independent review, or another provider may be unavailable in the area.
Sec. 9: Correction or Amendment of Information	Generally: Individuals should have the right to request correction or amendment of their information.	None.
Sec. 10: Notice of Information Practices	Generally: Holders of personal health information should provide notice of how they use the information and what rights an individual has.	Requirement may be too burdensome for some holders of information, particularly those who are outside the business of health care.
Sec. 11: Information Safeguards	Generally: Holders of personal health information should provide reasonable safeguards to protect the information.	None.

## HEALTH INFORMATION PRIVACY ACT, DRAFT 7/31/2000

<b>Section of Act</b>	<b>Area of Consensus</b>	<b>Area of Disagreement</b>
Sec. 12: Security Standards	Generally: Holders of personal health information should implement security standards to protect electronic transmission of data.	None.
Sec. 13: Complaint Procedures	Generally: Holders of personal health information should establish complaint procedures; an oversight agency also should provide an opportunity for addressing complaints.	This could be a costly requirement and add more bureaucratic layers.
Sec. 14: Authority of Department	Generally: An agency or public-private consortium should have authority to issue rules and monitor implementation of the legislative requirements.	Costly; no current agency appears to have sufficient expertise or staffing to handle this.
Sec. 15: Civil Penalty	Generally: Legislative requirements should be enforceable by civil action; violations should be subject to individual civil lawsuits for damages.	Some disagreement over the amount of damages and the civil penalty; also whether recovery of attorney fees should be mandatory or discretionary.
Sec. 16: Criminal Penalties	Generally: Violation of legislative requirements should be subject to criminal penalties.	Some disagreement over who should be subject to criminal penalties and at what level of complicity; concern that 1 <sup>st</sup> Amendment rights could be unlawfully infringed.
Sec. 17: Effect on Other State Laws	Generally: New legislative requirements should not impede or invalidate certain current situations requiring particular access to health information, such as public health or government data systems.	Some protections ought to apply even if a particular holder of health information should have freer rein than other holders.

# **ATTACHMENT 6**

## **SUMMARY of the DRAFT HEALTH INFORMATION PRIVACY ACT**

## ATTACHMENT 6

### SUMMARY of the DRAFT HEALTH INFORMATION PRIVACY ACT

The New Mexico Task Force on Health Data Privacy and Confidentiality developed the draft Health Information Privacy Act as a result of its work under House Joint Memorial 20 (1999). The Act reflects the Task Force's recommendations concerning the appropriate protection, access, use, disclosure and electronic transmission security standards of personal health data. The Act draws from the following sources:

- Health Insurance Portability and Accountability Act (1996);
- Recommendations of the Secretary of Health and Human Services on Confidentiality of Individually-Identifiable Health Information (1997);
- Department of Health and Human Services Proposed Rule on Standards for Privacy of Individually-Identifiable Health Information (1999); and
- Several model statutes on health information privacy.

Briefly, the Health Information Privacy Act:

- Creates a category of “protected health information” (health information that reveals, or could reasonably be expected to reveal, the identity of the individual) that is subject to restrictions on use and disclosure.
- Creates a category of “health information custodians” (health care providers, health care payers and others who obtain health information in the ordinary course of business) with responsibilities for safeguarding the confidentiality of protected health information and providing individuals access to their information.
- Prohibits the use or disclosure of protected health information except: (1) for purposes directly related to treatment, payment or health care operations; (2) for other, limited purposes specifically permitted by the Act; (3) as authorized by the individual; or (4) when otherwise required by law.
- Restricts all uses or disclosures of protected health information to the limited amount of information necessary to accomplish the intended purpose and to situations where non-protected information cannot be used instead.
- Prohibits health information custodians from redisclosing protected health information except as permitted by the Act or otherwise required by law.

- Requires health information custodians to maintain a record of disclosures of protected health information and permit individuals to inspect their disclosure record.
- Permits use and disclosure of protected health care information without individual authorization for specified purposes, such as public health, health system oversight, governmental health data collection, research with review board approval, emergencies, law enforcement activities, and when required by law.
- Allows individuals to authorize health information custodians to disclose their protected health information. Individuals must be informed of the intended use of the information and the right to revoke or amend the authorization.
- Creates a right for individuals to inspect, copy, correct and amend their protected health information, with limited exceptions, and file a statement of disagreement if a correction or amendment is refused. Individuals can request that the corrected or amended information, or the statement of disagreement, be provided to past recipients of the information.
- Requires health information custodians to prepare and disseminate a written notice of their information practices and the rights of individuals concerning their protected health information.
- Requires health information custodians to establish and maintain administrative, technical and physical safeguards to preserve the confidentiality, security, accuracy and integrity of protected health care information and guard against unauthorized access and other threats to security.
- Provides for the promulgation of security standards which health information custodians must implement for all electronically maintained or transmitted protected health information.
- Requires health information custodians to establish procedures for addressing complaints about the use or disclosure of protected health information, and requires a similar administrative process at the state level.
- Authorizes a designated agency or entity to promulgate rules and enforce the Act.
- Provides for civil enforcement and civil remedies, including damages and attorneys fees, for violation of the Act.
- Establishes criminal penalties for specified violations of the Act.
- Delineates the effect of the Act on other state laws.

**ATTACHMENT 7**

**TASK FORCE PROPOSED DRAFT LEGISLATION:  
HJM20**

**NOTE:**

*NOT ENDORSED BY:*

*THE NEW MEXICO HEALTH POLICY COMMISSION*

*SEPTEMBER 7, 2000*

BILL  
45TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2001  
INTRODUCED BY

DISCUSSION DRAFT

**FOR THE HOUSE JOINT MEMORIAL 20 (1999) TASK FORCE**

AN ACT

**RELATING TO HEALTH INFORMATION; ENACTING THE HEALTH INFORMATION PRIVACY ACT; LIMITING USE AND DISCLOSURE OF HEALTH INFORMATION; PROVIDING INDIVIDUAL RIGHTS; REQUIRING INFORMATION SAFEGUARDS; ESTABLISHING CIVIL AND CRIMINAL PENALTIES.**

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

**Section 1. SHORT TITLE.**--This act may be cited as the "Health Information Privacy Act".

**Section 2. PURPOSE OF ACT.**--The purpose of the Health Information Privacy Act is to protect the privacy of individually identifiable health information, control the use and disclosure of health information, provide individual rights of access and amendment of health information, and promote the efficient and secure transfer of health information for authorized purposes.

**Section 3. DEFINITIONS.**--As used in the Health Information Privacy Act:

- A. "disclose" means to release, transfer, transmit, publish, make available or otherwise divulge all or any part of protected health information;
- B. "electronically maintain" means to store information on a computer or on any electronic medium from which information may be retrieved by a computer;
- C. "electronically transmit" means to disclose information using a computer or other electronic media, but does not include radio communications;
- D. "health care" means:
  - (1) any preventive, evaluative, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, counseling, service or procedure with

respect to an individual's physical, mental or behavioral condition or functional status or that affects the structure or function of the human body or any part of the human body;

(2) any sale or dispensing of a drug, substance, device, equipment

or other item to an individual pursuant to a prescription; or

(3) any procurement or banking of blood, gametes, embryos,

organs, genetic materials or any other tissue for administration to individuals;

E. "health care clearinghouse" means a person that:

(1) facilitates the exchange and transfer of health information

between health information custodians;

(2) processes or facilitates the processing of health information

into a standard format for transfer and exchange between health information custodians;

or

(3) transforms protected health information into non-individually

identifiable health information;

F. "health care operations" means the following activities undertaken by or on behalf of a health care provider or health care payer for management or support of health care treatment or health care payment:

(1) quality assessment and improvement activities, including

outcomes evaluation and development of clinical guidelines;

(2) review or evaluation of the competence, qualifications or

performance of a health care provider or health care payer;

(3) supervised training of undergraduate and graduate students and

others in areas of health care to practice as health care providers;

(4) activities related to accreditation, certification, licensing or

credentialing;

(5) insurance rating and other insurance activities related to the renewal of a contract for insurance, including underwriting, experience rating and

reinsurance, but only when the individuals are already enrolled in a health plan conducting these activities and the use or disclosure of protected health information relates to an existing contract of insurance, including the renewal of a contract;

(6) medical review and auditing services, including fraud and abuse detection and compliance programs; or

(7) compilation and analysis of information in anticipation of or for use in a civil or criminal legal proceeding;

G. "health care payer" means a person that provides or pays all or part of the cost of health care treatment. "Health care payer" includes a government agency that administers a health care treatment program, but does not include an individual, or a family member or friend of the individual, who pays for his or her own health care treatment;

H. "health care provider" means a person that, with respect to a specific item of protected health information, receives, obtains, creates, uses, maintains or discloses the information while acting in whole or in part in the capacity of:

(1) a person who is licensed, certified, registered or otherwise authorized by law to provide health care treatment in the ordinary course of business or practice of a profession; or

(2) a person who provides services that are promoted to the public as health care treatment;

I. "health information" means any information, whether oral, written, electronic, visual, pictorial, physical or in any other form or medium, that relates to the past, present or future:

(1) physical, mental or behavioral health status or condition of an individual, including substance abuse;

(2) provision of health care treatment to the individual; or

(3) payment for the provision of health care treatment to the individual;

J. "health information custodian" means a person that receives, obtains, creates, uses, maintains or discloses protected health information in the ordinary course of business, regardless of whether receiving, obtaining, creating, using, maintaining or disclosing protected health information is the person's primary business. "Health information custodian" includes:

(1) a health care provider, health care payer, health care clearinghouse, third-party administrator of health care benefits, researcher, employer,

school or educational institution, financial institution, labor union, or any government agency or person that routinely receives, obtains, creates, uses, maintains or discloses protected health information in the ordinary course of business; and

(2) an officer, employee or agent of, or any person acting under grant of authority from or contract with, a person described in paragraph (1) of this subsection, including a person to whom the health information custodian discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the health information custodian;

K. "health oversight agency" means a government agency, or a person acting under grant of authority from or contract with a government agency, that performs or oversees the performance of an audit, investigation, inspection, licensure or discipline, civil, criminal or administrative proceeding, or other activity necessary for appropriate oversight of:

(1) the health care system;  
(2) government benefit programs for which health information is relevant to beneficiary eligibility; or  
(3) government regulatory programs for which health information is necessary for determining compliance with program standards;

L. "individual representative" means:

(1) a person legally empowered to make a health care decision for an individual who lacks capacity to make the decision, as provided in the Uniform Health Care Decisions Act, § 24-7A-1 to 24-7A-18, or other law;

(2) the personal representative, administrator or executor of the estate of a deceased individual; or

(3) a person authorized by law to act on behalf of a deceased individual;

M. "payment" means activities undertaken by or on behalf of a health care provider or health care payer to obtain reimbursement for the provision of health

care treatment, to obtain premiums, or to determine or fulfill responsibility for coverage and provision of benefits. "Payment" activities include:

(1) determinations of coverage, improving methods of paying for coverage, or adjudication or subrogation of health benefits claims;

(2) risk adjusting amounts due based on enrollee health status and demographic characteristics;

(3) billing, claims management, or medical data processing;

(4) review of health care services with respect to medical

necessity, coverage under a health plan, appropriateness of care, or justification of charges; or

(5) utilization review activities, including precertification or preauthorization of services;

N. "protected health information" means health information:

(1) that reveals the identity of the individual whose health care is the subject of the information; or

(2) where there is a reasonable basis to believe the information could be used to reveal the identity of the individual whose health care is the subject of the information, either by use of the information alone or with other information that should reasonably be known to be available to the predictable recipients of the health information;

O. "public health agency" means a government agency, or a person acting under grant of authority from or contract with a government agency, that is responsible for activities primarily aimed at the prevention of injury, disease, disability, or premature mortality or the promotion of health in the community through surveillance and epidemiological research, development of public health policy, response to public health needs and emergencies, and the collection of data on disease, injury and vital events such as birth or death;

P. "security standard" means a requirement, guideline or best practice designed to protect data privacy, integrity or availability; and

Q. "treatment" means:

(1) the provision of health care by a health care provider or the coordination of health care among health care providers, including risk assessment, case management or disease management for an individual;

(2) the referral of a patient from one health care provider to another; or

(3) the coordination of health care among health care providers and others authorized by the health care payer or individual.

**Section 4. GENERAL PROVISIONS ON USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION.--**

A. A health information custodian may use or disclose protected health information only as provided in the Health Information Privacy Act or otherwise required by law. Any other use or disclosure of protected health information by a health information custodian shall be prohibited.

B. A health information custodian shall not use or disclose protected health information when the use or disclosure is prohibited by the Health Information Privacy Act or other law.

C. A health information custodian may use and disclose protected health information as follows:

(1) for the provision of health care treatment to the individual whose health care is the subject of the information, to the extent the health information custodian or the recipient of the information engages in this activity;

(2) for payment for the provision of health care treatment to the individual whose health care is the subject of the information, to the extent the health information custodian or the recipient of the information engages in this activity;

(3) for health care operations, to the extent the health information custodian or the recipient of the information engages in these activities;

(4) as authorized by an individual whose health care is the subject of the information, in compliance with Section 7 of the Health Information Privacy Act;

or

(5) as permitted by and in compliance with Section 6 of the Health Information Privacy Act.

D. A health information custodian shall disclose protected health information as follows:

(1) to an individual whose health care is the subject of the protected health information, in compliance with Section 8 of the Health Information Privacy Act;

(2) to a person as requested by an individual whose health care is the subject of the protected information, in compliance with Section 7 of the Health Information Privacy Act; or

(3) as required by and in compliance with other law.

E. Any permitted or required use or disclosure of protected health information by a health information custodian shall be:

(1) directly related to the purpose for which use or disclosure of the protected health information is permitted or required;

(2) limited to the minimum amount of protected health information necessary to accomplish the intended purpose, to the extent reasonably practical; and

(3) restricted to situations where use of non-protected health information is not a reasonable alternative.

F. Nothing in the Health Information Privacy Act that permits a discretionary disclosure of protected health information shall be construed to require the disclosure, unless the disclosure is otherwise required by law.

G. Nothing in the Health Information Privacy Act shall be construed to prevent an individual from using or disclosing his or her protected health information in any way or to any person.

H. A health information custodian who obtains protected health information pursuant to the Health Information Privacy Act shall not use or redisclose the information except as provided by the Health Information Privacy Act or otherwise required by law.

I. A health information custodian shall comply with the provisions of the Health Information Privacy Act with respect to the protected health information of a

deceased individual for two years following the death of the individual. This requirement does not apply to uses or disclosures for research purposes.

J. The provisions of the Health Information Privacy Act shall not apply to protected health information of inmates in correctional facilities or detainees in detention facilities.

K. An individual representative may exercise the rights of an individual pursuant to the Health Information Privacy Act. If the individual is a minor and is authorized by law to consent to health care treatment without parental consent, only the minor may exercise the rights of an individual pursuant to the Health Information Privacy Act regarding the protected health information that relates to the health care treatment for which the minor lawfully consented.

#### **Section 5. DISCLOSURE HISTORY.--**

A. A health information custodian shall maintain a record of all disclosures of protected health information made by the health information custodian after the effective date of the Health Information Privacy Act, provided that:

(1) disclosures for the provision of health care treatment, health care payment or health care operations need not be recorded if the disclosure is confined to recipients within the health-related divisions of the health information custodian;

(2) disclosures made in accordance with a law that requires reporting of health information to a government agency need not be recorded; and

(3) a health care clearinghouse shall be exempt from maintaining a record of disclosures made for the provision of health care treatment or health care payment.

B. An individual shall be permitted to see the record of disclosures of the individual's protected health information, except for disclosures to a health oversight agency or law enforcement agency if the agency has provided to the health information custodian a written request that:

(1) states that the individual's access to the record of the disclosure would reasonably be likely to impede activities of the health oversight or law enforcement agency; and

(2) specifies the period of time for which the individual's access to the record of the disclosure should be denied.

C. The record of disclosures shall be retained for the life of the record to which it relates.

#### **Section 6. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION WITHOUT INDIVIDUAL AUTHORIZATION.--**

A. A health information custodian may use and disclose protected health information without individual authorization when necessary for providing health care treatment to the individual, for payment of health care treatment provided to the individual or for health care operations. An individual may request that disclosures for purposes of health care treatment or payment for health care treatment be limited to particular information or particular recipients. The health information custodian shall honor the individual's request and not make disclosures inconsistent with the limitations, except that disclosures permitted by this section or otherwise required by law shall not be subject to limitation by the individual.

B. A health information custodian may disclose protected health information without individual authorization to a public health agency authorized by law to obtain the information; a person authorized by law to obtain the information for compliance with the requirements or directions of a public health agency; or a person authorized by law to be notified in a public health intervention.

C. A health information custodian may disclose protected health information without individual authorization to a health oversight agency for oversight activities authorized by law.

D. A health information custodian may disclose protected health information without individual authorization to a government agency, or person acting under grant of authority from or contract with a government agency, for inclusion in a governmental health data system that collects and analyzes health data for policy, planning, regulatory or management functions authorized by law.

E. A health information custodian may disclose protected health information without individual authorization for research, provided that the health information custodian has obtained written documentation of the following:

(1) a waiver of the requirement to obtain individual authorization for use or disclosure of protected health information approved by either:

(a) an institutional review board established in accordance with federal law or regulations; or

(b) a research review board formally designated by a health information custodian that has members with varying backgrounds and appropriate professional competency as necessary to review the research protocol and ensure the protection of the rights and welfare of the research subjects; that is comprised at least fifty percent of members who are not affiliated with the entity conducting the research or related to a person who is affiliated with the entity; and that does not have any member participating in a review of any project in which the member has a conflict of interest;

(2) the approval is based on a determination and justification in writing by the institutional review board or research review board that waiver of the requirement to obtain individual authorization satisfies the following criteria:

(a) the research could not practicably be conducted without access to and use of the protected health information;

(b) the research could not practicably be conducted without the waiver;

(c) the use or disclosure of protected health information involves no greater probability or magnitude of anticipated harm or discomfort to the

research subjects than is ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests;

(d) the waiver will not adversely affect the rights and welfare of the research subjects;

(e) whenever appropriate, the research subjects will be provided with additional pertinent information after participation;

(f) the research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure;

(g) there is an adequate plan to protect the identifiers from improper use and disclosure; and

(h) there is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers; and

(3) the waiver contains the date of its approval by the institutional review board or research review board and is signed by the chair of the applicable board or the chair's designee.

F. A health information custodian may disclose protected health information without individual authorization based on a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any individual or the public, provided that disclosure may be made only to a person reasonably able to prevent or lessen the threat, including the target of the threat. A health information custodian shall be presumed to have acted on a reasonable belief if the disclosure is made in good faith based on either the information custodian's own knowledge and reasonable belief or on a credible representation by a person with apparent knowledge or authority.

G. A health care provider who provides health care treatment to an individual may disclose protected health information without individual authorization concerning the individual's current treatment to a family member or close personal friend of the individual under the following circumstances:

(1) the individual has agreed to the disclosure; or

(2) in circumstances where reasonable efforts have been made to obtain the individual's agreement to the disclosure but the individual's response cannot practicably or reasonably be obtained, only the protected health information that is directly relevant to the involvement of the family member or friend in the individual's health care is disclosed, consistent with good health professional practices and ethics.

H. A health care provider may disclose without individual authorization the fact of an individual's presence in a facility, the location of the facility, and the condition of the individual in general terms that do not reveal specific medical information about the individual, if the individual has not affirmatively objected in advance to this disclosure. Health care facilities shall provide individuals in their care with reasonable notice and opportunity to object to this type of disclosure.

I. A health information custodian may disclose protected health information without individual authorization to a law enforcement official if:

(1) the law enforcement official is conducting or supervising a law enforcement inquiry or proceeding authorized by law and the disclosure is pursuant to a

grand jury subpoena or a warrant, subpoena or order issued by a judicial officer that documents a finding by the judicial officer;

(2) the disclosure is for the purpose of identifying a suspect, fugitive, material witness or missing person and that individual's health care is the subject of the protected health information, provided that the disclosure shall be limited to the name, address, social security number, date and place of birth, type of injury or other distinguishing characteristic, and date and time of treatment of the individual;

(3) the disclosure is of protected health information of an individual who is or is suspected to be a victim of a crime, abuse or other harm, if:

(a) the law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred and immediate law enforcement activity that depends upon obtaining the information may be necessary; and

(b) reasonable efforts have been made to provide the victim an opportunity to consent to disclosure of all or part of the information and the victim has consented or is unable to consent; or

(4) the disclosure is to a law enforcement official reasonably able to act on the information and the health information custodian believes in good faith that the information disclosed constitutes evidence of criminal conduct that:

(a) arises out of and is directly related to receipt of health care treatment or payment for health care treatment, or qualification for or receipt of benefits, payments or services based on a fraudulent statement or material misrepresentation of the health of an individual;

(b) occurred on the premises of the health information custodian; or

(c) was witnessed by a member of the health information custodian's workforce.

J. A health information custodian may disclose protected health information concerning a deceased individual without individual authorization to a medical investigator or examiner to:

(1) identify the deceased individual; or

(2) determine a cause of death.

K. A health information custodian may disclose protected health information without individual authorization to a financial institution, or an entity engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting payments on behalf of a financial institution, if necessary for processing payments for health care treatment or health care premiums.

L. A health information custodian may disclose protected health information without individual authorization pursuant to a court order for the production or discovery of evidence.

M. A health information custodian may disclose protected health information as necessary in a claim or litigation between the individual whose health care is the subject of the information and the health information custodian.

N. A health information custodian shall disclose protected health information without individual authorization when required by other law and all the requirements of the other law are met.

**Section 7. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION WITH INDIVIDUAL AUTHORIZATION.--**

A. A health information custodian shall request and obtain authorization from an individual for all uses and disclosures of the individual's protected health information that:

(1) are not directly related to the provision of health care treatment to the individual, payment for the provision of health care treatment to the individual or health care operations;

(2) are not authorized by the individual whose health care is the subject of the information, in compliance with this section;

(3) are not permitted by and in compliance with Section 6 of the Health Information Privacy Act;

(4) are not required by and in compliance with

other law;

(5) involve use or disclosure of health information that is received or created by a health information custodian in the course of conducting research, for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care treatment and with respect to which the health information custodian has not requested payment from a third party payer;

(6) are for marketing of health and non-health items and services by the health information custodian;

(7) involve disclosure by sale, rental or barter;

(8) involve disclosure to non-health related divisions of the health information custodian;

(9) are to a health care provider or health plan, prior to an individual's enrollment in a health plan, for the purpose of making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating

determinations;

(10) are to an employer for use in employment determinations; or

(11) are for fundraising purposes.

B. An individual may request and authorize a health information custodian to disclose the individual's protected health information. The health information custodian shall honor the request and authorization.

C. An individual may revoke or amend an authorization to disclose protected health information at any time, except to the extent that the health information custodian has taken action in reliance on the authorization.

D. A health information custodian shall not condition the provision of health care treatment to an individual or payment for health care treatment on an individual's authorization of use or disclosure of protected health information, except where the authorization is requested in connection with the individual's participation in a clinical research trial.

E. An individual's authorization to use or disclose protected health information shall not be on the same document on which the individual consents to health care treatment; shall be in writing, dated and signed by the individual, or electronically authenticated; and shall include a description of the information to be disclosed, the identity of the intended recipient, the date or event by which the authorization expires, and a statement that the individual has the right to revoke or amend the authorization.

F. A health information custodian that requests an individual to authorize use or disclosure of protected health information shall provide a copy of the authorization to the individual. A health information custodian that discloses protected health information pursuant to an individual's authorization shall keep a copy of the authorization, or revocation or amendment of authorization, and a record of the disclosure.

G. A health information custodian may charge the individual a reasonable fee as reimbursement for the cost of retrieving and providing protected health information pursuant to the individual's request and authorization for disclosure.

#### **Section 8. INDIVIDUAL ACCESS TO PROTECTED HEALTH INFORMATION.--**

A. A health information custodian shall permit an individual to inspect and copy all or part of the individual's protected health information held by the health information custodian, except as provided in Subsection B of this section. Upon formal request from an individual, a health information custodian, as promptly as required under the circumstances but no later than thirty days after receiving the request, shall:

(1) make the information available for inspection during regular

business hours and, if requested, provide a copy to the individual in the form or format

specified by the individual, if the information is readily producible in that form or format;

(2) inform the individual if the information does not exist or cannot reasonably be found;

(3) provide the individual with the name and address of the person who maintains the record, if known, if the health information custodian does not maintain a record of the information;

(4) if the information is in use or unusual circumstances have delayed handling the request, provide the individual with a written statement in plain language that specifies the reasons for the delay and the earliest date, not later than forty-five days after receiving the request, when the information will be available for inspection or copying or when the request will be otherwise disposed of; or

(5) deny the request, in whole or in part, pursuant to Subsection B of this section; provide the individual with a written statement in plain language that specifies the basis for the denial; provide for inspection and copying of any portion of the request not denied, pursuant to Subsection C of this section; and, if applicable, provide for an independent review of the denied information, pursuant to Subsection D of this section.

B. A health information custodian may deny an individual's request to inspect and copy the individual's protected health information if the health information custodian reasonably believes that:

(1) inspection of the information could reasonably be expected to endanger the life or physical safety of any individual;

(2) inspection of the information could reasonably be expected to impede an ongoing health oversight or law enforcement activity;

(3) the information identifies or could reasonably lead to the identification of a person who provided the information under a promise of confidentiality to a health care provider, under circumstances in which confidentiality was appropriate;

(4) the information is used by the health information custodian solely for reasons other than providing health care treatment or other benefits to the individual; or

(5) inspection of the information is otherwise prohibited by law.

C. A denial of an individual's request to inspect and copy the individual's protected health information shall be limited to the minimum amount of protected health information necessary to effectuate the reason for the denial and the individual shall be permitted to inspect and obtain a copy of any portion of the requested information not subject to the denial.

D. A health information custodian that denies an

individual's request, in whole or in part, pursuant to paragraph (1) of Subsection B of this section, shall permit a health care provider selected by the individual to inspect the denied information and make an independent determination of whether the individual's request should be granted. The health information custodian shall inform the individual of the right to select a health care provider pursuant to this subsection.

E. A health information custodian may charge the individual a reasonable fee as reimbursement for the cost of retrieving and providing the requested protected health information.

**Section 9. CORRECTION OR AMENDMENT OF PROTECTED HEALTH INFORMATION.--**

A. For purposes of accuracy or completeness, an individual may request a health information custodian to correct or amend the individual's protected health information held by the health information custodian. Upon formal request from an individual, as promptly as required under the circumstances but no later than thirty days after receiving the request, the health information custodian shall:

(1) make the correction or amendment by adding the correction or amendment to the protected health information record, marking the challenged entries as corrected or amended and indicating the place in the protected health information record where the corrected or amended information is located; and inform the individual that the correction or amendment has been made;

(2) inform the individual if the information does not exist or cannot reasonably be found;

(3) provide the individual with the name and address of the person who maintains the record, if known, if the health information custodian does not maintain a record of the information;

(4) if the information is in use or unusual circumstances have delayed handling the request, provide the individual with a written statement in plain language that specifies the reasons for the delay and the earliest date, not later than forty-five days after receiving the request, when the correction or amendment will be made or when the request will be otherwise disposed of; or

(5) deny the request, in whole or in part, pursuant to Subsection B of this section.

B. A health information custodian may deny, in whole or in part, an individual's request for correction or amendment of the individual's protected health information if the health information custodian reasonably determines that the challenged

information is accurate and complete. A health information custodian who denies a request, in whole or in part, shall:

(1) provide the individual with a written statement in plain language that specifies the basis for the denial, informs the individual of the right to file with the protected health information custodian a concise, written statement of disagreement containing the requested correction or amendment and the individual's reasons for disagreeing with the denial, and informs the individual of the right to have the statement sent to past and future recipients of the protected health information, if requested by the individual;

(2) add the individual's statement of disagreement, if any, to the protected health information record, mark the challenged entry to indicate that the individual claims the entry is inaccurate or incomplete, and indicate the place in the protected health information record where the corrected or amended information is located, provided that the health information custodian may establish a limit to the length of the statement of disagreement and may summarize the statement of disagreement if necessary; and

(3) if the health information custodian so chooses, include as part of the protected health information record a concise statement of the health information custodian's reasons for not making the requested change.

C. A health information custodian that makes a correction or amendment or receives a statement of disagreement shall:

(1) make reasonable efforts to provide a copy of the corrected or amended protected health information or the statement of disagreement, including if it so chooses the health information custodian's concise statement of reasons for not making the requested change, to persons who previously received the uncorrected or unamended information, as requested by the individual; and

(2) in the event of a disputed correction or amendment of the protected health information, include a copy of the individual's statement of disagreement, including if it so chooses the health information custodian's concise statement of reasons for not making the requested change, in any subsequent disclosure

of the disputed portion of the information.

D. A person who receives a correction or amendment of an individual's protected health information, or a statement of disagreement, from a health information custodian concerning previously received uncorrected or unamended protected health information shall have no obligation to take action on the correction or amendment unless requested by the individual or as otherwise required by law.

E. A health information custodian may charge the individual a reasonable fee as reimbursement for the cost of retrieving, correcting, amending and disseminating the individual's protected health information as requested, or for disseminating the individual's statement of disagreement with the refused correction or amendment, unless an error by the health information custodian caused the need for the correction or amendment.

#### **Section 10. NOTICE OF INFORMATION PRACTICES.--**

A. A health information custodian, other than a health care clearinghouse, shall prepare a written notice in plain language to inform individuals of the health information custodian's information practices and the individuals' rights regarding protected health information.

B. A health care provider shall:

(1) include in the notice an explanation of:

(a) the uses and disclosures of protected health information authorized by the Health Information Privacy Act;

(b) the uses and disclosures of protected health information intended by the health care provider;

(c) the right of the individual to prevent or limit disclosure of protected health information as provided in the Health Information Privacy Act;

(d) the right of the individual to inspect and copy protected health information and to request corrections or amendments;

(e) the procedures for authorizing disclosure and for revoking authorization for disclosure of protected health information;

(f) the procedures for the exercise and redress of rights under the Health Information Privacy Act; and

(g) the fees, if any, to be charged to the individual for inspection, copying, distribution or provision of protected health information;

(2) provide a copy of the written notice to individuals whose protected health information is held by the health care provider, either by giving each individual a copy of the written notice, regardless of request, ninety days after the effective date of the Health Information Privacy Act or by advising each individual of the availability of the written notice at the first service delivery after the effective date of the Health Information Act and providing a copy on request; and

(3) post a copy of the notice in a clear and prominent location where it is reasonable to expect that individuals seeking service from the health care provider will be able to read the notice.

C. A health care payer shall:

(1) include in the notice an explanation of the information required in paragraph (1) of Subsection B of this section, as consistent with the provisions of the Patient Protection Act, § 59A-57-1 to 59A-57-11; and

(2) provide a copy of the written notice to individuals whose protected health information is held by the health care payer by giving each individual then enrolled or covered by the health care payer a copy of the written notice ninety days after the effective date of the Health Information Privacy Act and providing a copy to subsequently-enrolled or covered individuals at the time of enrollment or coverage.

D. A health information custodian other than a health care provider or health care payer shall:

(1) include in the notice an explanation of:

(a) the uses and disclosures of protected health information authorized by the Health Information Privacy Act;

(b) the uses and disclosures of protected health information intended by the health information custodian;

(c) the right of the individual to prevent or limit disclosure of protected health information as provided in the Health Information Privacy Act;

(d) the procedures for authorizing disclosure and for revoking authorization for disclosure of protected health information; and

(e) the procedures for the exercise and redress of rights under the Health Information Privacy Act; and

(2) provide a copy of the notice upon request to individuals whose protected health information is held by the health information custodian.

E. A health information custodian shall not use or disclose protected health information in a manner inconsistent with the notice. A health information custodian that revises its information practices in a manner inconsistent with the notice shall provide a revised notice to individuals, in the manner specified in this section, within thirty days of the revision. Where posting of the notice is required, a revised notice shall be posted within thirty days of the revision.

#### **Section 11. INFORMATION SAFEGUARDS.--**

A. A health information custodian shall establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to:

(1) ensure the confidentiality, security, accuracy, and integrity of protected health information in its possession;

(2) protect against reasonably anticipated threats or hazards to the security or integrity of protected health information in its possession; and

(3) protect against unauthorized use or disclosure of protected health information in its possession.

B. A health information custodian shall periodically assess potential risks and vulnerabilities to the protected health information in its possession and implement, maintain and document security measures necessary to protect the privacy of the information as required by the Health Information Privacy Act.

C. A health information custodian shall implement, maintain and document the security standards promulgated in accordance with Section 12 of the Health Information Privacy Act for all protected health information that the health information custodian electronically maintains or electronically transmits.

#### **Section 12. SECURITY STANDARDS.--**

A. The [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium] shall develop and promulgate security standards to protect the confidentiality, integrity and availability of protected health information that is electronically maintained or electronically transmitted.

B. The security standards shall comply with state and federal information security standards and shall include the following features:

(1) administrative procedures to manage the implementation of security measures and the conduct of personnel in relation to the protection of data;

(2) physical safeguards to protect computer systems and related equipment and buildings from intrusion, fire and other natural and environmental hazards;

(3) technical security services to protect information and control authorized access to information; and

(4) technical security mechanisms to guard against unauthorized access to data that is transmitted over a communications network.

C. The [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium] shall establish an advisory committee to assist it in developing and periodically reviewing health data security standards. The advisory committee shall consist of representatives of public and private health information custodians, state agencies that electronically maintain or electronically transmit protected health information, consumers, and professionals with expertise in areas such as information systems and data security. The advisory committee shall make recommendations to the [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium] on:

(1) appropriate security standards for protected health information that is electronically maintained or electronically transmitted;

(2) implementation of security standards, including time requirements and phase-in options, if any; and

(3) review and revision of security standards.

#### **Section 13. COMPLAINT PROCEDURES**

A. A health information custodian shall establish and maintain procedures, in accordance with requirements promulgated by the [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium], for adequately addressing complaints by individuals concerning the use or

disclosure of their protected health information by the health information custodian or their rights under the provisions of the Health Information Privacy Act.

B. The [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium] shall establish administrative procedures for addressing complaints from individuals concerning the use or disclosure of their protected health information by a health information custodian or their rights under the provisions of the Health Information Privacy Act.

**Section 14. AUTHORITY OF DEPARTMENT.--**

A. The [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium] shall have authority to promulgate rules to implement the provisions of the Health Information Privacy Act.

B. The [Human Services Department, Department of Health, Health Policy Commission or a public/private consortium] shall have authority to:

- (1) independently monitor compliance with Section 11 and Section 12 of the Health Information Privacy Act;
- (2) inspect documentation of security standards and require additional documentation;
- (2) inspect a health information custodian's data systems and premises;
- (4) receive reports of violations of Section 11 or Section 12 of the Health Information Privacy Act; and
- (5) order corrective measures.

**Section 15. CIVIL PENALTIES.--**

A. The attorney general or district attorney may bring a civil action against a health information custodian for violating the provisions of the Health Information Privacy Act or to otherwise enforce those provisions.

B. A person whose protected health information has been wrongfully used or disclosed or whose rights under the provisions of the Health Information Privacy Act have been violated may bring a civil action against a health information custodian for damages or other relief.

C. The court may order a health information custodian who violates the provisions of the Health Information Privacy Act to comply with those provisions and may order any other appropriate relief, including:

- (1) damages for economic and non-economic loss;
- (2) damages of up to five thousand dollars (\$5,000) in addition to any economic and non-economic loss if the violation results from willful or grossly negligent conduct;
- (3) a civil penalty of not more than one thousand dollars (\$1,000) per violation if the violation results from willful or grossly negligent conduct; and
- (4) reasonable attorney fees and appropriate court

costs.

D. In an action by an individual alleging that protected health information was improperly withheld from the individual pursuant to Section 8 of the Health Information Privacy Act, the burden of proof is on the health information custodian to prove that the information was properly withheld.

E. A health information custodian that discloses protected health information pursuant to an individual's authorization that has been revoked or amended shall not be subject to liability or penalty under the Health Information Privacy Act if the health information custodian had no actual or constructive notice of the revocation or amendment at the time the information was disclosed.

F. The court may use protected health information to determine the cause of damage or injury and award appropriate relief.

G. Each instance of wrongful use or disclosure of protected health information, or wrongful denial of an individual's rights under the provisions of the Health Information Privacy Act, constitutes a separate and actionable violation of the Health Information Privacy Act.

H. The provisions of this section do not affect the rights and remedies available to an individual under other law.

#### **Section 16. CRIMINAL PENALTIES.--**

A. A health information custodian who knowingly uses or discloses protected health information in violation of the Health Information Privacy Act is guilty of a misdemeanor and shall be punished by a fine of not more than one thousand dollars (\$1,000) or imprisonment for a definite term not to exceed one year, or both.

B. A health information custodian who knowingly uses or discloses protected health information under false pretenses or with the intent to sell or transfer the information for commercial advantage, personal gain or malicious harm in violation of the Health Information Privacy Act is guilty of a fourth degree felony and shall be punished by a fine of not more than five thousand dollars (\$5,000) or imprisonment for a definite term not to exceed eighteen months, or both.

#### **Section 17. EFFECT ON OTHER STATE LAWS.--**

A. Nothing in the Health Information Privacy Act shall be construed to invalidate or limit the authority, power or procedures established under any law providing for:

- (1) reporting of disease or injury, child abuse or neglect, adult abuse or neglect, or birth, death or other vital events;
- (2) public health surveillance, investigation or intervention.
- (3) a governmental health data system that collects and analyzes

health data for policy, planning, regulatory or management functions authorized by law.

B. [Amendment or repeal of inconsistent state laws.]

C. The provisions of the Health Information Privacy Act shall prevail over any other contrary provision of state law, except that a contrary provision of state law shall prevail over a provision of the Health Information Privacy Act if with respect to individually identifiable health information the contrary provision of state law requires:

- (1) more limited use or disclosure of the information (in terms of the number of potential recipients of the information, the amount of information to be disclosed, or the circumstances under which information may be disclosed);
- (2) greater rights for individuals to access or amend their information;

(3) greater penalties for unlawful use or disclosure of the information;

(4) a more detailed explanation to be provided to an individual about a proposed use or disclosure of information, the rights of the individual, the availability of remedies or similar issues;

(5) a narrower scope or shorter duration of individual authorization for use or disclosure of information, or procedures that increase the difficulty of obtaining individual authorization or reduce the coercive effect of the circumstances surrounding the authorization;

(6) the retention or reporting of more detailed information or for a longer duration; or

(7) greater privacy protection for the individual with respect to any other related matter.

**Section 18. SEVERABILITY.--**If any part or application of the Health Information Privacy Act is held invalid, the remainder or its application to other situations or persons shall not be affected.

**Section 19. EFFECTIVE DATE.--**The effective date of the provisions of this act is July 1, 2001. [Or assume the usual 90 days after legislative adjournment.]