State Regulation of Health Information: Arizona and Nevada

Kristen B. Rosati, Esq.

Coppersmith Gordon Schermer Owens & Nelson PLC
Phoenix, Arizona

HIPAA Summit West
June 22, 2001

Overview

- HIPAA preemption: how does it work?
- Preemption examples from Arizona and Nevada
- HIPAA compliance efforts in Arizona and Nevada
- Gramm-Leach-Bliley implementation in Arizona and Nevada

©Coppersmith Gordon

HIPAA Preemption

- Standards preempt "contrary" provision of state law (with certain exceptions)
  - Contrary: Cannot comply with both state and federal requirement or state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of HIPAA

©Coppersmith Gordon

HIPAA Preemption

- What is a provision of state law?
  - Constitution, statute, regulation, rule, common law (court cases), or "other State action having the force and effect of law"
  - Carefully examine non-regulatory state agency action (such as Department of Insurance circulars or agency statements of policy)

©Coppersmith Gordon

HIPAA Does Not Preempt:

- State law provision (including state procedures established under such law) that provides for reporting of disease or injury, child abuse, birth or death, or for conducting public health surveillance, investigation or intervention

©Coppersmith Gordon

Preemption Exceptions cont . . .

- State law provision requires health plans to report, or to provide access to, information for purpose of management or financial audits, program monitoring or evaluation, or licensure and certification of facilities or individuals

©Coppersmith Gordon

Preemption Exceptions cont. . .

- State law provision relates to the privacy of health information (it has the specific purpose of protecting the privacy of health information or it affects the privacy of health information in a direct, clear and substantial way); and
- State law provision is "more stringent"

©Coppersmith Gordon

What Is "More Stringent"?

- Regarding use or disclosure
  - State law provision prohibits or restricts the use or disclosure in circumstances under which such use or disclosure would be permitted under HIPAA (unless the disclosure is required by the Secretary in connection with determining HIPAA compliance or the disclosure is to the individual who is the subject of the individually identifiable health information (IIHI))

©Coppersmith Gordon

What Is "More Stringent"?

- Regarding the right to access or amend
  - State law provision provides greater rights of access or amendment, except that the HIPAA regulations do not preempt any state law to the extent it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor

©Coppersmith Gordon

What Is "More Stringent"?

- Regarding information provided to an individual about a use or disclosure of his or her IIHI, or the individual's rights and remedies
  - State law provision provides a greater amount of information to the individual

©Coppersmith Gordon

What Is "More Stringent"?

- Regarding the form or substance of an authorization or consent for use or disclosure of IIHI
  - State law provision provides requirements that narrow the scope or duration of the use or disclosure, increase the privacy protections afforded to the individual (such as by expanding the criteria for the authorization or consent), or reduce the coercive effect of the circumstances surrounding the authorization or consent

©Coppersmith Gordon

What Is "More Stringent"?

- Regarding record keeping or requirements relating to accounting of disclosures
  - State law provision requires reporting of more detailed information or retention for a longer duration
- Regarding any other matter
  - State law provision provides greater privacy protection for the individual who is the subject of the IIHI

©Coppersmith Gordon

Preemption Exceptions cont. . .

- Secretary determines that necessary:
  - To prevent fraud or abuse related to the provision of or payment for health care
  - To ensure state regulation of insurance or health plans, to extent authorized by law
  - For state reporting on health care delivery or costs
  - For purposes of serving compelling need relating to public health, safety or welfare (if HHS determines the intrusion to privacy is warranted when balanced against the need for the information)
  - For improving Medicare or Medicaid program or the efficiency of the health care system

©Coppersmith Gordon

Preemption Exceptions cont. . .

- Secretary determines the state law provision has the principle purpose of addressing the manufacture, registration, distribution, dispensing or other control of controlled substances

©Coppersmith Gordon

How Does HHS Determine Preemption?

- Anyone (not just states) may request determination of whether state law provision preempted
  - Preemption determination effective until Secretary revokes the exception or until law changes so that ground for exception no longer exists
- No advisory opinions as to whether state law is preempted because it is "more stringent," etc.

©Coppersmith Gordon

Examples of Preemption Analysis

- Arizona statute requiring child abuse reporting, ARS § 13-3620
  - Is any provision within the statute "contrary" to the HIPAA regulations?
  - Does it provide for reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention?

©Coppersmith Gordon

Examples of Preemption Analysis

- Nevada statute requiring reporting of contagious diseases, NRS § 441A.150
  - Is any provision within the statute "contrary" to the HIPAA regulations?
  - Does it provide for reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention?

©Coppersmith Gordon

Examples of Preemption Analysis

- Arizona statute regarding release of records to third parties: A.R.S. § 12-2294
  - Is any provision within the statute "contrary" to the HIPAA regulations?
  - Does it provide for reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention?
  - Does it require health plans to report or provide access to information for listed purposes?

©Coppersmith Gordon

Examples of Preemption Analysis

- Evaluation of A.R.S. § 12-2294 continued:
  - Does it relate to the privacy of health information?
  - Is it "more stringent" than the HIPAA regulations?

©Coppersmith Gordon

Examples of Preemption Analysis

- Nevada health care records statute, NRS § 629.061:
  - Is any provision within the statute "contrary" to the HIPAA regulations?
  - Does it provide for reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention?
  - Does it require health plans to report or provide access to information for listed purposes?

©Coppersmith Gordon

Examples of Preemption Analysis

- Evaluation of NRS § 629.061 continued:
  - Does it relate to the privacy of health information?
  - Is it "more stringent" than the HIPAA regulations?

©Coppersmith Gordon

Arizona HIPAA Compliance Efforts

- Arizona Hospital and Healthcare Association (AzHHA) HIPAA Task Force
- AzHHA Arizona law preemption analysis
- AzHHA Consent Manual revision to incorporate HIPAA

©Coppersmith Gordon

Nevada HIPAA Compliance Efforts

- Conversations with Nevada providers and regulators did not reveal state-wide HIPAA compliance efforts
- Audience discussion—are HIPAA compliance coordination efforts underway?

©Coppersmith Gordon

©Coppersmith Gordon

Gramm-Leach-Bliley Implementation in Arizona

- Ariz. SB 1288 (1st Reg. Session 2001)
  - Amends existing law (A.R.S. § 20-2101 et seq.) requiring insurance companies to give notice of information practices to applicants and policy holders
  - Notice must contain G-L-B- elements or state statutory elements
  - May give notice to sponsor of employee benefit plan (not individual) if no disclosure of individual information made other than those allowed by § 20-2113

Gramm-Leach-Bliley Implementation in Arizona

- SB 1288 continued . . .
  - Numerous disclosures allowed under § 20-2113 without individual authorization (some of which will be preempted by HIPAA)
  - Enforcement by Department of Insurance
  - Effective date of new legislation: August 9, 2001
  - No regulations contemplated

©Coppersmith Gordon

©Coppersmith Gordon

Gramm-Leach-Bliley Implementation in Arizona

- FTC Regulations (65 Fed. Reg. 33646)
  - Apply to ERISA plans (self-funded group health plans)
    - FTC regs provide that no notice is required to individual, just to plan sponsor
  - Apply to all other entities defined as "financial institutions" and not regulated by state insurance department (accounting firms, law firms in some circumstances, etc.)
  - Implementation date July 1, 2001

Gramm-Leach-Bliley Implementation in Nevada

- Nevada AB 618: Section 135 of bill requires compliance by insurance licensees with G-L-B- Title V and provides that violation is an unfair trade practice
- Nevada Financial Privacy Proposed Temporary Regulation: July 1, 2001 compliance date

©Coppersmith Gordon

Questions?

Kristen Rosati
Coppersmith Gordon
Schermer Owens & Nelson PLC
2633 E. Indian School Rd., Suite 300
Phoenix, Arizona 85016
Kristen@cgson.com
602-381-5464

State Regulation of Health Information: Arizona and Nevada

Exhibit 1
HIPAA Privacy:
The Compliance Challenges Ahead

Coppersmith Gordon Schermer Owens & Nelson PLC
Attorneys and Counselors
2633 East Indian School Road, Suite 300
Phoenix, Arizona 85016-6759
Tel (602) 224-0999 · fax (602) 224-6020

HIPAA Privacy: The Compliance Challenges Ahead

Executive Summary

On December 28, 2000, the U.S. Department of Health and Human Services published the long-awaited final Standards for Privacy of Individually Identifiable Health Information ("Privacy Standards") under the Health Insurance Portability and Accountability Act. The Privacy Standards will have a profound effect on how health care providers, health plans, and health care clearinghouses do business. The Privacy Standards:

- Comprehensively regulate the internal use and external disclosure of "protected health information," creating rules for when patient consent or authorization is required for use and disclosure, and what that consent or authorization must contain;
- Create individual patient rights to inspect and copy patient's own protected health information, to amend erroneous or incomplete information, to obtain an "accounting" of disclosures of information, to request restrictions of uses or disclosures for treatment, payment or health care operations, to receive confidential communications, and to receive notice of an institution's privacy practices;
- Establish a number of administrative requirements, including requiring institutions to have an extensive set of policies to protect the privacy of health information, to appoint a "privacy official" to develop those policies, and to conduct workforce training on those policies; and
- Mandate contracts with "business associates" to ensure that they also protect health information.

When Must Your Organization Comply with the Privacy Standards?

Health care providers, health care clearinghouses, and most health care plans must comply by **April 14, 2003**, 24 months after the effective date of the regulations. "Small" health plans—those with less than $5 million in annual receipts—must comply by April 14, 2004.

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

WHY DID DHHS ISSUE THE PRIVACY STANDARDS?

HIPAA, a statute passed by Congress in 1996, included the "Administrative Simplification" provisions, calling for the adoption of national standards to facilitate the electronic exchange of health information to make financial and administrative health care transactions more efficient.

The government calculates that national standards for the electronic exchange of health information (the "**standard transactions**") are expected to result in huge savings for the health care industry: $29.9 billion over the next ten years. These savings result from a reduction in time to process claims, elimination of lost paper claims, improvement in data quality, and a significant reduction in operating costs due to reduction in manual data entry. Moreover, providers who already transmit electronic claims to health plans are expected to save because these providers will not have to maintain multiple proprietary EDI formats. On August 17, 2000 DHHS published regulations implementing these standard transactions, called the Standards for Electronic Transactions.

Encouraging this electronic transmission of health information, however, may lead to widespread dissemination of this private and sensitive information. As DHHS has noted, "the same technological advances that make possible enormous administrative cost savings for the industry as a whole have also made it possible to breach the security and privacy of health information on a scale that was previously inconceivable." In HIPAA, Congress called for the issuance of regulations to protect the privacy and security of personal health information.

The resulting regulations, the Privacy Standards, impose strict requirements on the use and disclosure of individual health information. At the same time, DHHS recognized that providers and payers must have prompt access to complete medical information. DHHS attempted to balance these concerns in the Privacy Standards; whether DHHS achieved this goal is debatable. One thing is certain: the Privacy Standards will impose substantial expense and operational changes on the health care industry. The government estimates the cost of implementing the Privacy Standards at $17.6 billion over ten years; the American Hospital Association's estimate comes in much higher at $22 billion over five years.

DHHS plans to issue additional regulations to implement the remaining Administrative Simplification provisions. We expect DHHS to issue the final Security Standards this spring, which will govern covered entities' computer system and physical plant security. In addition, DHHS will issue regulations governing national "identifiers" assigned to various participants in the health care system, such as providers, health plans, and employers. National identifiers for individuals are on hold due to the controversy spurred by that proposal.

THE FINAL PRIVACY STANDARDS: A SUMMARY

This newsletter is designed to provide a bird's-eye view of the Privacy Standards. You should consult the text of the actual Privacy Standards or legal counsel before designing your policies and procedures.

Is Your Organization a "Covered Entity"?

Your organization will be required to comply with the Privacy Standards if it is a health plan, a health care clearinghouse, or a health care provider that transmits health information electronically in connection with a standard transaction, such as an electronic claim for payment. Your organization also will be required to comply if it instructs other entities (such as third party billing companies or health care clearinghouses) to submit electronic claims or other standard transactions on its behalf. Organizations (and individuals) required to comply with the Privacy Standards are called "**covered entities**."

If a provider does not submit electronic claims and does not participate in any other standard transaction, that provider will not have to comply with the Privacy Standards.

If your organization is a "hybrid entity," that is, your organization is a covered entity whose primary function is not as a health care provider,

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

health care plan, or health care clearinghouse, then the "health care component" of your organization must comply with the Privacy Standards. However, the hybrid entity itself still has some limited responsibilities. If your organization falls within this category, please read the regulations carefully or consult your legal counsel.

What Type of Information Is Protected by the Standards?

If your organization is a covered entity, the Privacy Standards protect all "**individually identifiable health information**" your organization handles.

ALERT: The final Privacy Standards protect paper records, oral communications, and information transmitted or maintained electronically. This is a substantial change from the proposed regulations, which protected only electronic information.

Information is not "individually identifiable" if a person with appropriate statistical knowledge concludes the risk is very small that the information could be used to identify an individual, or if the "identifiers" listed in the regulations are removed (such as names, geographic designations, dates of service, telephone, fax, addresses, URLs and IP addresses, biometrics, photographs, and other identifying information).

Organizations can "de-identify" information by removing, coding, encrypting or concealing specified information that would lead to identifying an individual. If health information is not "individually identifiable," that information is not protected by the Privacy Standards.

Use and Disclosure of Protected Health Information

The Privacy Standards comprehensively regulate the internal use and external disclosure of protected health information, creating complicated rules for when patient consent or authorization is required for use and disclosure, and what that consent or authorization must contain.

How can your organization use and disclose protected health information?
The Privacy Standards divide use and disclosure into five categories: (1) required disclosures; (2) uses and disclosures where patient "consent" is required for treatment, payment and health care operations; (3) uses and disclosures where patient "authorization" is required; (4) uses and disclosures for which the individual must be given an opportunity to object or agree; and (5) uses and disclosures for which no consent, authorization, or opportunity to object is required.

1. Required Disclosures: The Standards require only two types of disclosures:

- Disclosure to the Secretary of DHHS to investigate compliance with the Privacy Standards;
- Disclosure to an individual of his or her own protected health information.

2. Patient "Consent" Required: Treatment, Payment and Health Care Operations: A health care provider may use or disclose a patient's protected health information to treat that patient, to obtain payment for that treatment, or to carry out "health care operations," only if it first obtains patient "**consent.**"

Interestingly, other covered entities may use health information for treatment, payment, or health care operations without patient consent.

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

What are health care operations? These activities include a wide range of day-to-day activities, such as quality assessment and improvement, case management and care coordination, review of the competence or qualifications of health care professionals and practitioners, conduct of training programs, accreditation, certification, licensing, credentialing, underwriting and premium rating, obtaining legal services, auditing, business planning, and other administrative activities.

Exceptions to Consent: Providers do not need to obtain consent in the following situations:

- The provider must use the information for emergency treatment, if the provider attempts to obtain consent as soon as possible;
- The provider is required by law to treat the individual, attempts to obtain consent, but is unable to do so;
- The provider is unable to obtain consent due to substantial communication barriers and concludes that the consent to receive treatment can be inferred from the circumstances;
- The provider has an "indirect treatment relationship" with the patient, where the provider delivers health care to the patient based on the orders of another provider, and where the provider typically provides the services or reports the diagnosis or results to the other provider; or
- The provider created or received the information in the course of treating an inmate.

Consent Form Requirements: The Privacy Standards contain detailed requirements for consent forms. Be careful to include each of the required elements in your consent form, or the patient's consent will not be valid. Patient consent <u>can</u> be a condition of treatment or payment.

Previous Consents: Providers may use or disclose protected health information under consents and authorizations obtained before the Privacy Standards' compliance date, even if the consent or authorization does not meet the new regulatory requirements. However, the previously obtained consent or authorization applies only to protected health information created or received before the compliance date.

3. Patient "Authorization" Required:

The Privacy Standards require "authorization" for any use or disclosure of information that is not otherwise explicitly required or permitted by the Privacy Standards. For example, an organization may not sell or rent patient information without obtaining the patient's authorization. In addition, a provider generally must obtain patient authorization to use or disclose psychotherapy notes.

<u>ALERT</u>: Patient "authorization" is different from "consent," and must contain more details concerning the use or disclosure proposed. Unlike "consent," situations, providers and health plans may <u>not</u> condition treatment, payment or enrollment on the individual's "authorization" to use or disclose information.

Fundraising and Marketing: In general, organizations may not use protected health information in fundraising and marketing without patient authorization. However, the regulations allow the use of patient demographic information and dates of treatment in fundraising activities if organizations include notice of this practice in their privacy notices. In some circumstances, organizations also may use protected health information for limited marketing without individual authorization. In both situations, the patient must be given the opportunity to "opt-out" of future solicitations.

4. Opportunity to Object or Agree Required:

In two limited circumstances, the regulations allow an organization to use and disclose information without patient consent or authorization, as long as the organization gives the patient advance notice of the use or disclosure and the opportunity to object, or "opt-out" of the use or disclosure:

- Providers may include a patient's name, location in the facility, condition in general terms (as long as it does not communicate specific medical information), and religious

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

affiliation in facility directories. They may disclose this information to anyone who asks for the individual by name, except that religious affiliation may be disclosed only to clergy members; and
- Any covered entity may disclose to family members and others involved in a person's care, information directly relevant to the patient's care or information or to notify them of the patient's location and condition. Different rules apply when the patient is present and able to consent and when the patient is not present or incapable of consenting.

The organization may inform the patient orally of this use or disclosure and obtain the patient's oral agreement.

5. Patient Consent, Authorization, or Opportunity to Object Not Required:

The Privacy Standards allow the use and disclosure of protected health information in a variety of circumstances where that information is essential for public purposes or for the operation of the health care system. Patient consent, authorization, or opportunity to object is not required where the disclosure is:

- Required by law;
- For certain public health activities;
- About victims of abuse, neglect or domestic violence;
- For health oversight activities;
- For judicial and administrative proceedings;
- For certain law enforcement purposes;
- To coroners, medical examiners and funeral directors about deceased persons;
- For cadaveric organ, eye or tissue donation purposes;
- For research;
- To avert a serious threat to health or safety;
- For specialized government functions, such as military and veterans activities, national security and intelligence, protective services for the President, correctional institutional custodial situations, or government programs providing public benefits; and
- For workers' compensation.

ALERT: For use and disclosure without consent, authorization, or opportunity to object, the Privacy Standards contain many detailed requirements. Check the actual regulatory language before releasing any information.

The Minimum Necessary Standard:

When organizations use or disclose protected health information, or request protected health information from another covered entity, they must make reasonable efforts to limit the information to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

For routine disclosures of information, your organization can establish a protocol to determine what is "minimally necessary"; for all other disclosures, your organization must make an individual determination about whether each proposed disclosure is the minimum necessary information.

For internal uses of information, your organization must determine which persons or classes of persons in its workforce need access to protected health information and the categories of information to which they need access. No individual "minimum necessary" determination is required for internal use.

Exceptions to the Minimum Necessary Standard: This Standard does not apply to disclosures:

- To a health care provider for treatment;
- To the individual of his or her own information;
- To the Secretary of DHHS to investigate compliance;
- As required by law; and
- As required for compliance with the Privacy Standards.

Individual Rights

The Privacy Standards also create a number of individual patient rights:

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

Right to Inspect and Copy Information: Patients will have the right to access and copy their own protected health information maintained in "designated record sets." A designated record set includes medical records and billing records maintained by a provider; enrollment, payment, claims adjudication, and case or medical management records systems maintained by a health plan; or records that are used by any covered entity to make decisions about an individual. Thus, individuals are not entitled to information contained in providers' peer review or quality assurance files.

A few types of information are exempt from inspection and copying, including psychotherapy notes, information compiled in anticipation of legal proceedings, and information that may not be disclosed to individuals under the Clinical Laboratory Improvements Amendments (lab results reported to providers). Moreover, the regulations provide other limited circumstances in which an organization may deny access to an individual, such as where provision of that information would pose a danger to the patient or to others.

An organization must respond to an individual's request for access within 30 days under most circumstances, and must provide a process for the individual to challenge most denials of access.

Right to Amend Information: Individuals also will have the right to amend erroneous or incomplete protected health information, unless the information was not created by the covered entity, is not in a "designated record set," is accurate and complete, or would not be available for inspection under the previous section.

An organization must respond within 60 days by granting or denying the request, and must follow the procedures set forth in the regulations. If the covered entity denies the request, an individual may file a statement of disagreement (and the covered entity a rebuttal statement), all of which must be included in the patient's record.

ALERT: Amendment of health information has serious risk management implications, particularly for medical malpractice actions. Be sure to consult risk management personnel or legal counsel before granting an amendment request.

Right to Receive Accounting of Disclosures: Individuals also will have the right to obtain an "accounting" of disclosures of their protected health information made within six years before the request, starting at the compliance date (February 26, 2003 for most covered entities). This accounting must include disclosures made by both the covered entity and its business associates.

The organization must respond within 60 days of the request, and must include a number of elements in the accounting.

Disclosures exempt from the accounting requirement include those:

- To carry out treatment, payment, and health care operations;
- To individuals of their own information;
- For the facility's directory;
- To family members and others involved in the individual's care;
- For national security or intelligence purposes; and
- To correctional institutions and other law enforcement agencies under the custodial exception.

Right to Request Restriction of Use or Disclosure: Individuals have the right to request restrictions on how covered entities will use or disclose their protected health information for treatment, payment or health care operations, and how their information will be disclosed to family members or others involved in their care. A covered entity is not required to agree to such a restriction; however, if the covered entity agrees, it must comply with that agreement.

Right to Receive Confidential Communications. A health care provider must accommodate reasonable requests by individuals to receive communications of protected

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

health information by alternative means or at alternative locations.

Right to Receive Notice of Privacy Practices: An individual has the right to receive a notice of an organization's privacy practices that describes its uses and disclosures of protected health information, the individual's rights under the Privacy Standards, and the organization's legal duties regarding protected health information. This notice must be in plain language and contain specific elements prescribed by the regulations.

Draft the Notice of Privacy Practices Carefully! Your organization may use or disclose information only in compliance with its notice, even if the notice is more restrictive than the regulations. Moreover, if your organization wants to change the privacy practices described by its notice, it must first publish a revised notice. If an organization does not reserve the right to change its practices in its privacy notice, any change in practices can only apply to protected health information received after publication of the new notice. This privacy notice must be drafted very carefully to ensure the greatest amount of flexibility for the organization.

Administrative Requirements

The Privacy Standards also impose a number of administrative requirements on covered entities.

Policies and Procedures: The Privacy Standards will require your organization to have an extensive set of policies and procedures to protect the privacy of health information. These policies and procedures should take into account the size and type of activities at the organization. DHHS will expect to see more comprehensive privacy policies at larger health care institutions or health plans.

An organization may not make a change to its policies and procedures that materially affect the content of its notice of privacy practices, until it revises its notice.

Designation of "Privacy Official": Organizations must designate a "privacy official" who is responsible for the development and implementation of the privacy policies and procedures. Not every organization will need a new FTE for this purpose; small providers may wish to delegate these responsibilities to an existing employee.

Designation of Contact Person to Receive Complaints: Organizations must provide a process for individuals to complain about their privacy policies or violations of those policies. Each organization must designate a person or official responsible for receiving complaints under the Privacy Standards and who can provide further information about the matters discussed in the privacy notice. An organization may not require individuals to waive their right to complain as a condition of treatment, payment, or enrollment.

Workforce Training and Sanctions: Organizations must train all members of the workforce on their privacy policies and procedures "as necessary and appropriate for the members of the workforce to carry out their function." This training must take place by the compliance date and every time the privacy practices change materially. In addition, an organization must have and apply appropriate sanctions against its workforce members who fail to comply with its policies.

Disclosure Safeguards: Organizations must have in place administrative, technical, and physical safeguards to protect the privacy of health information against any intentional or unintentional use or disclosure of information. When DHHS issues the Security Standards, presumably during the Spring of 2001, those regulations will provide details concerning required safeguards.

Mitigation: Organizations must do what they can to mitigate any harmful effect that results from a use or disclosure of protected health information by them or their business associates, which is in violation of its policies or the Privacy Standards.

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

Refraining from Intimidating or Retaliatory Acts: Organization may not "intimidate, threaten, coerce, discriminate against, or take other retaliatory actions against" an individual for exercising his or her rights under the Privacy Standards or against any person who files a complaint with the Secretary of DHHS, who participates in an investigation, or who opposes any unlawful practice.

Documentation: The Privacy Standards require organizations to maintain written or electronic copies of its policies and procedures and of any written communication (such as consents and authorizations) required by the Standards. An organization must maintain that documentation for six years.

Business Associates

DHHS does not have the statutory authority to regulate people and companies not defined as "covered entities" under the regulations (such as employers, life insurance companies, copy services, and others). However, the Privacy Standards require covered entities to regulate them through the "business associate" provisions.

Who is a business associate? Simply put, a business associate is a person or company who performs an activity for a covered entity that involves the use or disclosure of individually identifiable health information or any other function regulated by the Privacy Standards.

Examples of business associates are firms conducting claims processing or administration; data analysis; processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; or legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Who is not a business associate? Members of the organization's workforce are not business associates. In addition, covered entities participating in "organized health care arrangements" (such as clinically integrated care settings or a health system in which more than one entity participates) are not business associates of each other simply because they provide services to the arrangement.

The Preamble to the Privacy Standards clarifies that health care providers and health care plans are not business associates of each other, because health care plans do not perform an activity on behalf of the provider. Similarly, a medical staff member is not a business associate of the hospital at which he or she holds privileges.

When can a covered entity disclose protected health information to a business associate? Covered entities can disclose protected health information to a business associate when use or disclosure is permitted by the Privacy Standards.

In addition, covered entities must have written contracts or agreements with business associates (**"business associate contracts"**) to ensure that each associate protects such health information.

Exceptions where business associate contracts are not required:

- **Where an organization discloses information to a health care provider concerning treatment;**
- **By a group health plan to a plan sponsor under certain circumstances;**
- **To a government agency determining eligibility for a health plan, if it is not the same agency that is administering the plan.**

What must a business associate contract include? A business associate contract must contain provisions that establish the permitted and required uses and disclosures for protected health information. Business associate contracts also must provide, among other things, that the business associate may not use or further disclose the information other than as permitted by the contract or as required by law, must ensure their agents and subcontractors comply with the same restrictions, must report any violations to the covered entity, and must make their practices and records available for inspection by the Secretary of DHHS. Significantly, at the termination of the contract

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

the business associate must return or destroy all protected health information, if feasible.

ALERT: The Privacy Standards contain numerous requirements for drafting business associate contracts. Review the regulations carefully or consult legal counsel.

STATE LAW APPLICATION

The Privacy Standards generally preempt all "contrary" state law, where it is impossible to comply with both the state law and the Privacy Standards. However, there are exceptions where even contrary state law will continue to apply:

- The state law relates to the privacy of health information and is "more stringent" (i.e. it is more favorable in some way to the patient);
- The state law provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation or intervention;
- The state law requires a health plan to report or to provide access to information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals; and
- The Secretary of DHHS determines that the state law is necessary to prevent fraud and abuse; to ensure state regulation of insurance and health plans; to serve a compelling public need related to public health, safety or welfare; or that the State law relates to controlled substances.

ENFORCEMENT

Why should your organization comply with the Privacy Standards, particularly when compliance will be very expensive? Of course, stringent patient privacy protection is good business and may help your organization avoid lawsuits for violation of privacy rights. Equally as important, HIPAA violations can result in both civil and criminal penalties.

Civil Penalties: HIPAA provides civil penalties of $100 per violation up to $25,000 per year for all violations of an "identical" requirement or prohibition. This may add up quickly to substantial penalties. Thankfully, the Privacy Standards contain a number of limitations on civil penalties. First, DHHS cannot impose a civil penalty if the act or omission is criminally punishable (scant comfort to those prosecuted, of course). In addition, DHHS cannot impose a civil penalty if the person can prove to DHHS's satisfaction that he or she did not know or by exercising reasonable diligence would not have known that he or she violated the Privacy Standards. Finally, DHHS cannot impose a civil penalty if the failure was due to reasonable cause and is not a result of willful neglect, and where the failure to comply is corrected within 30 days of the date the organization knew or should have known of the violation.

Criminal Penalties: HIPAA also provides for referral for criminal charges against a person who knowingly and in violation of the law obtains or discloses individually identifiable health information. Penalties are graduated into three levels of severity:

- For "basic" offenses, a maximum fine of $50,000 and up to one year in prison;
- For offenses committed under false pretenses, a maximum fine of $100,000 and up to five years in prison; and
- For offenses committed with intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a maximum fine of $250,000 and up to ten years prison.

Cooperation and Assistance: The Privacy Standards state that the Secretary will seek the cooperation of a covered entity in complying with the Privacy Standards, and may provide technical assistance to help organizations comply voluntarily with the Standards. In exchange, covered entities must cooperate with complaint investigations and compliance reviews.

Complaint Investigations: Any person who believes an organization is not complying with the Privacy Standards may file a written complaint with the Secretary of DHHS within 180 days of when the person knew or should have known of the violation. The Secretary then may investigate the complaint by reviewing an organization's policies, procedures, or practices

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

and the circumstances regarding the alleged violation.

Compliance Reviews: An organization must keep records and produce compliance reports as required by the Secretary to determine whether the organization is complying. An organization must cooperate with periodic compliance reviews, and must permit access by Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information. If access to information is controlled by another entity that refuses to produce, an organization must certify its efforts to obtain the information.

Resolution of Investigation: If a complaint investigation or compliance review reveals a violation, the Secretary will inform the organization (and the individual making the complaint) and attempt to resolve the matter informally. The Privacy Standards are unclear whether such "informal" resolutions are in the nature of a financial settlement or whether the Secretary will take a more benign approach, particularly in the initial years of enforcement. If the dispute cannot be resolved informally, the Secretary may issue written findings documenting noncompliance and may initiate civil or criminal action.

Enforcement Agencies: The Secretary of DHHS has delegated civil enforcement responsibility to the Director of the DHHS Office of Civil Rights. The FBI presumably will handle criminal investigations.

No Private Cause of Action: HIPAA does not authorize a private cause of action. Moreover, the provision in the proposed regulations that required business partner contracts to make patients third-party beneficiaries is not found in the final Privacy Standards. Thus, no *federal* cause of action exists for violation of patient's privacy rights.

However, private litigants could attempt to bring state claims for violation of privacy rights, "reliance" claims based on violation of the organization's notice of privacy practices, or claims under state consumer protection statutes.

TACKLING COMPLIANCE IN YOUR ORGANIZATION

The Privacy Standards are an extremely large, complicated set of regulations. Where should your organization's compliance efforts begin? We suggest the following initial compliance steps:

- Set up a HIPAA compliance task force within your organization. Ensure that this task force has cross-departmental representation (if applicable), including personnel from compliance, information technology, health information management, billing, medical and clinical departments, risk management, human resources, and legal. Your organization should not treat HIPAA compliance as just a technology issue! These regulations will affect almost every aspect of your organization.
- Educate key players about the Privacy Standards. Begin with the individuals on your HIPAA compliance task force, but expand to educate key management and clinical personnel. Also, be sure to educate your organization's Board members—they have a fiduciary responsibility to ensure that your organization is HIPAA-compliant by the enforcement date.
- Set a budget for your initial compliance activities.
- Assess how your organization uses and discloses protected health information, including how your existing policies and procedures protect health information.
- Evaluate the security of your computer system and physical plant.
- Based on this assessment and evaluation, develop a detailed implementation plan, with interim milestones, to address the "gaps" found in your analysis.
- Identify your business associates and educate them about the Privacy Standards. Involve in-house or outside legal counsel to evaluate existing and future contracts with all business associates.
- Hire or designate your privacy official. While the privacy official's primary duty must be to develop your organization's policies and procedures to protect health information, consider giving other duties to the privacy official, such as conducting employee education, undertaking privacy audits, and

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

functioning as a patient and government liaison. Cross-departmental authority and direct reporting to high-level administration is essential for the privacy official's successful implementation of your organization's HIPAA compliance.

- Begin developing your policies and procedures, and try out those new practices well before your organization is required to issue its notice of privacy practices.

WHERE CAN YOU GET MORE INFORMATION?

A number of Web Sites contain helpful information on the Privacy Standards. These include:

- **Department of Health and Human Services, Administrative Simplification Web Site:** http://aspe.hhs.gov/admnsimp/. This site contains general information about the HIPAA Administrative Simplification provisions, the proposed and final regulations, public comments submitted to DHHS, and updates on when HIPAA standards may be implemented.
- **American Hospital Association:** http:/www.aha.org/. The AHA Web Site contains good background materials for education.
- **Arizona Hospital and Healthcare Association:** http://www.azhha.org
- **Workgroup for Electronic Data Interchange (WEDI):** http://www.wedi.org/.
- **Association for Electronic Health Care Transactions:** http://www.afehct.org/.
- **Health Financial Management Association:** http://www.hfma.org/
- **American Health Information Management Association:** http://www.ahima.org/
- **National Association of Insurance Commissioners:** http://www.naic.org/
- **Healthcare Information and Management Systems Society:** http://www.himss.org/
- **American Medical Informatics Association:** http://www.amia.org/index.html
- **American Medical Association:** http://www.ama-assn.org/

For more information on our HIPAA legal services, please feel free to contact Kristen Rosati of Coppersmith Gordon Schermer Owens & Nelson P.L.C., at 602-381-5464; kristen @cgson.com, or any other CGSON lawyer at the numbers below.

Samuel G. Coppersmith	602-381-5461	sam@cgson.com
Andrew S. Gordon	602-381-5460	andy@cgson.com
Beth J. Schermer	602-381-5462	beth@cgson.com
Karen C. Owens	602-381-5463	karen@cgson.com
Julie M. Nelson	602-381-5465	julie@cgson.com
Kristen B. Rosati	602-381-5464	kristen@cgson.com
Sarah E. Porter	602-381-5466	sarah@cgson.com
Joseph A. Mislove	602-381-5475	joe@cgson.com
Michael K. Ben-Horin	602-381-5476	mike@cgson.com
James D. Jorgensen	602-381-5478	jamie@cgson.com

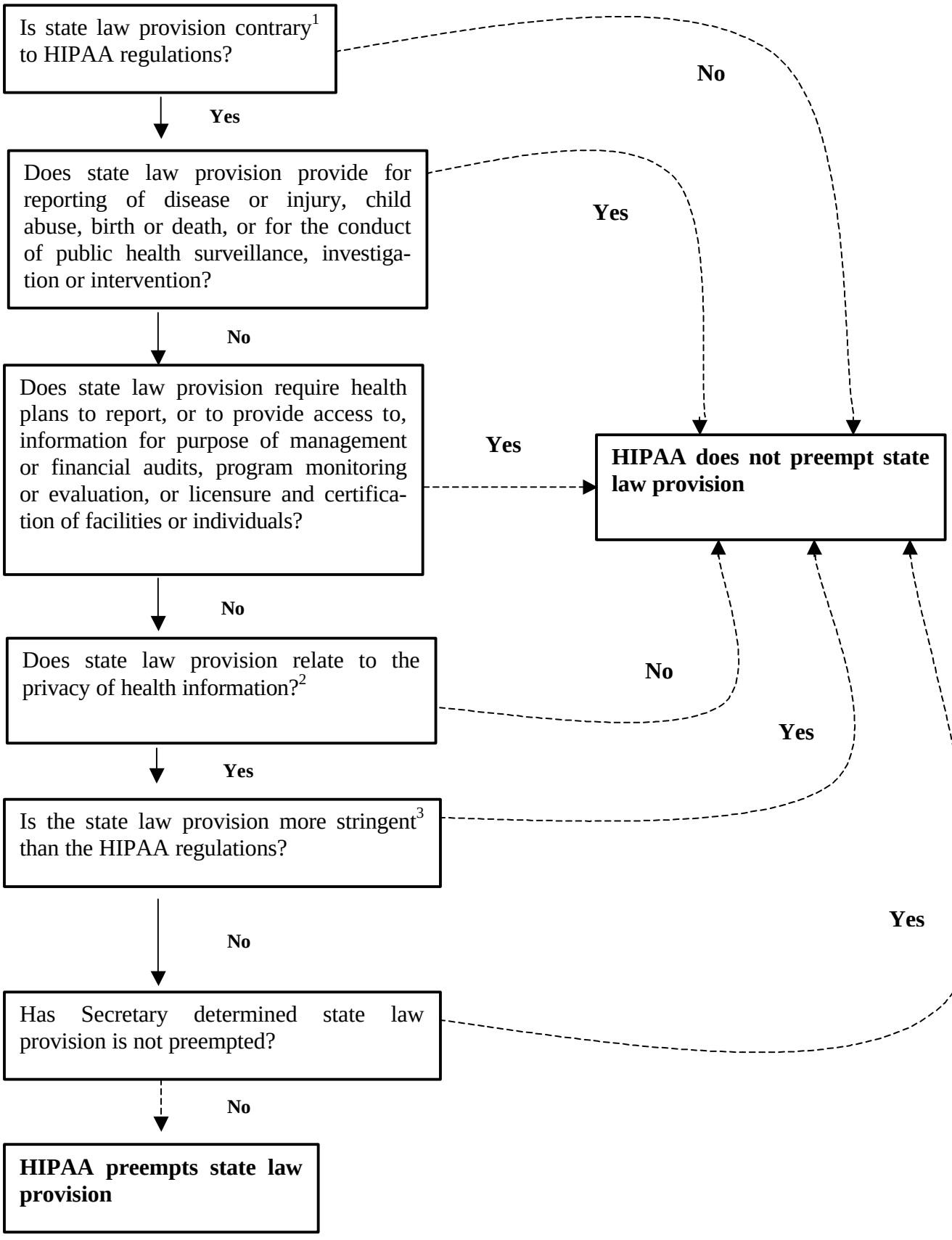
This article is intended only to serve as a practical guide and to provide general information. It is not intended as legal or other professional advice, and the authors are not rendering legal or other professional advice through this article. If you require legal advice or other expert assistance, please seek the services of an attorney or other appropriate professional.

©2001 Coppersmith Gordon Schermer Owens & Nelson PLC. Reproduction with attribution permitted.

State Regulation of Health Information: Arizona and Nevada

Exhibit 2
HIPAA Preemption Analysis Flowchart

HIPAA Preemption Analysis Flowchart



[1] *"Contrary" means* "(1) A covered entity would find it impossible to comply with both the State and federal requirements; or (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable."

[2] *"Relates to the privacy of individually identifiable health information"* means "that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way."

[3] *"More stringent"* means, "a State law that meets one or more of the following criteria: (1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is: (i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or (ii) To the individual who is the subject of the individually identifiable health information. (2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor. (3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information. (4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable. (5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration. (6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

State Regulation of Health Information: Arizona and Nevada

Exhibit 3
Examples of HIPAA Preemption: Arizona and Nevada State Laws

EXAMPLES FOR HIPAA PREEMPTION ANALYSIS

Arizona Revised Statutes, Section 13-3620. Duty and authorization to report nonaccidental injuries, physical neglect and denial or deprivation of necessary medical or surgical care or nourishment of minors; duty to make medical records available; exception; violation; classification

A. Any physician, hospital intern or resident, surgeon, dentist, osteopath, chiropractor, podiatrist, county medical examiner, nurse, psychologist, school personnel, social worker, peace officer, parent, counselor, clergyman or priest or any other person having responsibility for the care or treatment of children whose observation or examination of any minor discloses reasonable grounds to believe that a minor is or has been the victim of injury, sexual abuse pursuant to section 13-1404, sexual conduct with a minor pursuant to section 13-1405, sexual assault pursuant to section 13-1406, molestation of a child pursuant to section 13-1410, commercial sexual exploitation of a minor pursuant to section 13-3552, sexual exploitation of a minor pursuant to section 13-3553, incest pursuant to section 13-3608 or child prostitution pursuant to section 13-3212, death, abuse pursuant to section 8-201, or physical neglect which appears to have been inflicted on that minor by other than accidental means or which is not explained by the available medical history as being accidental in nature or who has reasonable grounds to believe there has been a denial or deprivation of necessary medical treatment or surgical care or nourishment with the intent to cause or allow the death of an infant less than one year of age protected under section 36-2281 shall immediately report or cause reports to be made of this information to a peace officer or to child protective services in the department of economic security. A clergyman or priest who has received a confidential communication or a confession in that person's role as a clergyman or a priest in the course of the discipline enjoined by the church to which the clergyman or priest belongs may withhold reporting of the communication or confession if the clergyman or priest determines that it is reasonable and necessary within the concepts of the religion. This exemption applies only to the communication or confession and not to personal observations the clergyman or priest may otherwise make of the minor. A report is not required under this section for conduct prescribed by sections 13-1404 and 13-1405 if the conduct involves only minors age fourteen, fifteen, sixteen or seventeen and there is nothing to indicate that the conduct is other than consensual. Reports shall be made forthwith by telephone or in person forthwith and shall be followed by a written report within seventy-two hours. The reports shall contain:

1. The names and addresses of the minor and the minor's parents or the person or persons having custody of the minor, if known.

2. The minor's age and the nature and extent of the minor's injuries or physical neglect, including any evidence of previous injuries or physical neglect.

3. Any other information that the person believes might be helpful in establishing the cause of the injury or physical neglect.

B. A health care professional who is regulated pursuant to title 32 and whose routine newborn physical assessment of a newborn infant's health status or whose notification of

positive toxicology screens of a newborn infant gives the professional reasonable grounds to believe that the newborn infant may be affected by the presence of alcohol or a substance prohibited by chapter 34 of this title shall immediately report this information, or cause a report to be made, to child protective services in the department of economic security. For the purposes of this subsection "newborn infant" means a newborn infant who is under thirty days of age.

C. Any person other than one required to report or cause reports to be made in subsection A of this section who has reasonable grounds to believe that a minor is or has been a victim of abuse or neglect may report the information to a peace officer or to child protective services in the department of economic security.

D. A person having custody or control of medical records of a minor for whom a report is required or authorized under this section shall make the records, or a copy of the records, available to a peace officer or child protective services worker investigating the minor's neglect or abuse on written request for the records signed by the peace officer or child protective services worker. Records disclosed pursuant to this subsection are confidential and may be used only in a judicial or administrative proceeding or investigation resulting from a report required or authorized under this section.

E. When such telephone or in-person reports are received by the peace officer, they shall immediately notify child protective services in the department of economic security and make the information available to them. Notwithstanding any other statute, when child protective services receives these reports by telephone or in person, it shall immediately notify a peace officer in the appropriate jurisdiction.

F. Any person required to receive reports pursuant to subsection A of this section may take or cause to be taken photographs of the child and the vicinity involved. Medical examinations including, but not limited to, radiological examinations of the involved child may be performed.

G. A person furnishing a report, information or records required or authorized under this section, or a person participating in a judicial or administrative proceeding or investigation resulting from a report, information or records required or authorized under this section, shall be immune from any civil or criminal liability by reason of such action unless the person acted with malice or unless the person has been charged with or is suspected of abusing or neglecting the child or children in question. Except as provided in subsection H of this section, the physician-patient privilege, the husband-wife privilege or any privilege except the attorney-client privilege, provided for by professions such as the practice of social work or nursing covered by law or a code of ethics regarding practitioner-client confidences, both as they relate to the competency of the witness and to the exclusion of confidential communications, shall not pertain in any civil or criminal litigation or administrative proceeding in which a child's neglect, dependency, abuse or abandonment is an issue nor in any judicial or administrative proceeding resulting from a report, information or records submitted pursuant to this section nor in any investigation of a child's neglect or abuse conducted by a peace officer or child protective services in the department of economic security.

H. In any civil or criminal litigation in which a child's neglect, dependency, abuse or abandonment is an issue, a clergyman or priest shall not, without his consent, be examined as a witness concerning any confession made to him in his role as a clergyman or a priest in the course of the discipline enjoined by the church to which he belongs. Nothing in this subsection discharges a clergyman or priest from the duty to report pursuant to subsection A of this section.

I. If psychiatric records are requested pursuant to subsection D of this section, the custodian of the records shall notify the attending psychiatrist, who may excise from the records, before they are made available:

1. Personal information about individuals other than the patient.

2. Information regarding specific diagnosis or treatment of a psychiatric condition, if the attending psychiatrist certifies in writing that release of the information would be detrimental to the patient's health or treatment.

J. If any portion of a psychiatric record is excised pursuant to subsection I of this section, a court, upon application of a peace officer or child protective services worker, may order that the entire record or any portion of the record containing information relevant to the reported abuse or neglect be made available to the peace officer or child protective services worker investigating the abuse or neglect.

K. A person who violates this section is guilty of a class 1 misdemeanor.

Nevada Revised Statutes Section 441A.150. <u>Reporting occurrences of communicable diseases to health authority</u>.

1. A provider of health care who knows of, or provides services to, a person who has or is suspected of having a communicable disease shall report that fact to the health authority in the manner prescribed by the regulations of the board. If no provider of health care is providing services, each person having knowledge that another person has a communicable disease shall report that fact to the health authority in the manner prescribed by the regulations of the board.

2. A medical facility in which more than one provider of health care may know of, or provide services to, a person who has or is suspected of having a communicable disease shall establish administrative procedures to ensure that the health authority is notified.

3. A laboratory director shall, in the manner prescribed by the board, notify the health authority of the identification by his medical laboratory of the presence of any communicable disease in the jurisdiction of that health authority. The health authority shall not presume a diagnosis of a communicable disease on the basis of the notification received from the laboratory director.

4. If more than one medical laboratory is involved in testing a specimen, the laboratory that is responsible for reporting the results of the testing directly to the provider of health care for the patient shall also be responsible for reporting to the health authority.

Arizona Revised Statutes Section 12-2294. Release of medical records to third parties

A. A health care provider shall disclose medical records or the information contained in medical records without the patient's written authorization as otherwise required by law.

B. A health care provider may disclose medical records or the information contained in medical records without the patient's written authorization as follows or as otherwise authorized by law:

1. To attending and consulting health care providers who are currently providing health care to the patient for the purpose of diagnosis or treatment of the patient.

2. To health care providers who have previously provided treatment to the patient, to the extent that the records pertain to the provided treatment.

3. To ambulance attendants as defined in section 36-2201 for the purpose of providing care to or transferring the patient whose records are requested.

4. To a private agency that accredits health care providers and to the allopathic board of medical examiners.

5. To health care providers for the purpose of conducting utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

6. To a person or entity that provides billing, claims management, medical data processing, utilization review or other administrative services to the patient's health care providers.

7. To the legal representative of a health care provider in possession of the medical record for the purpose of securing legal advice.

8. To the personal representative or administrator of the estate of a deceased patient. If a personal representative or administrator has not been appointed, a health care provider may release medical records to the following persons and in the following order of priority, unless the deceased patient during the deceased patient's lifetime or a person in a higher order of priority has notified the health care provider in writing that he opposes the release of the medical records:

(a) The deceased patient's spouse, unless the patient and the patient's spouse were legally separated at the time of the patient's death.

(b) The acting trustee of a trust created by the deceased patient either alone or with the deceased patient's spouse if the trust was a revocable inter vivos trust during the deceased patient's lifetime and the deceased patient was a beneficiary of the trust during his lifetime.

(c) An adult child of the deceased patient.

(d) A parent of the deceased patient.

(e) An adult brother or sister of the deceased patient.

(f) A guardian or conservator of the deceased patient at the time of the patient's death.

9. To the patient's third party payor if the payor has separately obtained the patient's written authorization to disclose medical record information to the payor and furnishes a copy of this authorization to the health care provider.

C. In addition to the persons listed in subsection B, paragraph 8 of this section, a health care provider may release medical records or the information contained in medical records to the patient's health care decision maker at the time of the patient's death.

D. A health care provider shall disclose medical records to persons listed in subsection B, paragraphs 2, 4, 5 and 8 of this section only on written request. The person requesting the records shall sign the request and shall demonstrate the authority to have access to the records.

E. Medical records that are not in written form shall only be released if the written request specifically identifies the type of record desired.

F. Medical records that are disclosed pursuant to this section remain privileged. A person who receives medical records pursuant to this section shall not disclose those records without the written authorization of the patient or the patient's health care decision maker, unless otherwise provided by law.

Nevada Revised Statutes Section 629.061. Health care records: Inspection; use in public hearing; immunity of certain persons from civil action for disclosure.

1. Each provider of health care shall make the health care records of a patient available for physical inspection by:

(a) The patient or a representative with written authorization from the patient;

(b) An investigator for the attorney general or a grand jury investigating an alleged violation of NRS 200.495, 200.5091 to 200.50995, inclusive, or 422.540 to 422.570, inclusive;

(c) An investigator for the attorney general investigating an alleged violation of NRS 616D.200, 616D.220, 616D.240 or 616D.300 to 616D.440, inclusive, or any fraud in the administration of chapter 616A, 616B, 616C, 616D or 617 of NRS or in the provision of benefits for industrial insurance; or

(d) Any authorized representative or investigator of a state licensing board during the course of any investigation authorized by law.

The records must be made available at a place within the depository convenient for physical inspection, and inspection must be permitted at all reasonable office hours and for a reasonable length of time. If the records are located outside this state, the provider shall make any records requested pursuant to this section available in this state for inspection within 10 working days after the request.

2. The provider of health care shall also furnish a copy of the records to each person described in subsection 1 who requests it and pays the actual cost of postage, if any, the costs of making the copy, not to exceed 60 cents per page for photocopies and a reasonable cost for copies of X-ray photographs and other health and care records

produced by similar processes. No administrative fee or additional service fee of any kind may be charged for furnishing such a copy.

3. Each person who owns or operates an ambulance in this state shall make his records regarding a sick or injured patient available for physical inspection by:

(a) The patient or a representative with written authorization from the patient; or

(b) Any authorized representative or investigator of a state licensing board during the course of any investigation authorized by law.

The records must be made available at a place within the depository convenient for physical inspection, and inspection must be permitted at all reasonable office hours and for a reasonable length of time. The person who owns or operates an ambulance shall also furnish a copy of the records to each person described in this subsection who requests it and pays the actual cost of postage, if any, and the costs of making the copy, not to exceed 60 cents per page for photocopies. No administrative fee or additional service fee of any kind may be charged for furnishing a copy of the records.

4. Records made available to a representative or investigator must not be used at any public hearing unless:

(a) The patient named in the records has consented in writing to their use; or

(b) Appropriate procedures are utilized to protect the identity of the patient from public disclosure.

5. Subsection 4 does not prohibit:

(a) A state licensing board from providing to a provider of health care or owner or operator of an ambulance against whom a complaint or written allegation has been filed, or to his attorney, information on the identity of a patient whose records may be used in a public hearing relating to the complaint or allegation, but the provider of health care or owner or operator of an ambulance and his attorney shall keep the information confidential.

(b) The attorney general from using health care records in the course of a civil or criminal action against the patient or provider of health care.

6. A provider of health care or owner or operator of an ambulance, his agents and employees are immune from any civil action for any disclosures made in accordance with the provisions of this section or any consequential damages.

State Regulation of Health Information: Arizona and Nevada

Exhibit 4
Gramm-Leach-Bliley Act Implementation
Arizona Senate Bill 1288

House Engrossed Senate Bill

State of Arizona
Senate
Forty-fifth Legislature
First Regular Session
2001

SENATE BILL 1288

AN ACT

AMENDING SECTIONS 20-2101, 20-2104 AND 20-2113, ARIZONA REVISED STATUTES; AMENDING TITLE 20, CHAPTER 11, ARTICLE 1, ARIZONA REVISED STATUTES, BY ADDING SECTION 20-2121; RELATING TO INSURANCE INFORMATION PRIVACY.

(TEXT OF BILL BEGINS ON NEXT PAGE)

Be it enacted by the Legislature of the State of Arizona:

Section 1. Section 20-2101, Arizona Revised Statutes, is amended to read:

20-2101. Scope

A. ~~The obligations imposed by~~ This chapter ~~apply~~ APPLIES to ~~those~~ insurance institutions, agents or insurance support organizations ~~which, on or after the effective date of this chapter~~ THAT:

1. In the case of life, health or disability insurance~~,~~ EITHER:

(a) Collect, receive or maintain information in connection with insurance transactions ~~which~~ THAT pertain to natural persons who are residents of this state ~~or~~.

(b) Engage in insurance transactions WITH applicants, individuals or policyholders who are residents of this state.

2. In the case of property or casualty insurance~~,~~:

(a) Collect, receive or maintain information in connection with insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state ~~or~~.

(b) Engage in insurance transactions involving policies, contracts or certificates of insurance delivered, issued for ~~deliveries~~ DELIVERY or renewed in this state.

B. The rights granted by this chapter extend to:

1. In the case of life, health or disability insurance, the persons who are residents of this state, including natural persons who are the subject of information collected, received or maintained in connection with insurance transactions ~~involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state~~, and applicants, individuals or policyholders who engage in or seek to engage in insurance transactions ~~involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state~~.

2. In the case of property or casualty insurance, the persons, including natural persons who are the subject of information collected, received or maintained in connection with insurance transactions INVOLVING POLICIES, CONTRACTS OR CERTIFICATES OR INSURANCE DELIVERED, ISSUED FOR DELIVERY OR RENEWED IN THIS STATE, and applicants, individuals or policyholders who engage in or seek to engage in insurance transactions INVOLVING POLICIES, CONTRACTS OR CERTIFICATES OF INSURANCE DELIVERED, ISSUED FOR DELIVERY OR RENEWED IN THIS STATE.

C. For purposes of this section, a person is considered a resident of this state if the person's last known mailing address, as shown in the records of the insurance institution, agent or insurance support organization, is located in this state.

D. Notwithstanding subsections A and B, this chapter does not apply to information collected from the public records of a governmental authority and maintained by an insurance institution or its representatives for the purpose of insuring the title to real property located in this state.

Sec. 2. Section 20-2104, Arizona Revised Statutes, is amended to read:

20-2104. Notice of insurance information practices

A. An insurance institution or agent shall provide a notice of information practices to ~~all~~ applicants AND ~~or~~ policyholders in connection with insurance transactions as PRESCRIBED IN THIS SECTION. ~~provided under the following:~~

B. THE INSURANCE INSTITUTION OR AGENT SHALL PROVIDE THE NOTICE AT THE FOLLOWING TIMES:

1. In the case of an application for insurance, ~~a notice no~~ NOT later than ~~at the time of the delivery of~~ EITHER WHEN THE INSURANCE INSTITUTION OR AGENT:

(a) DELIVERS the insurance policy or certificate, if personal information is collected only from the applicant or from public records~~, or at the time the collection of~~.

(b) FIRST COLLECTS personal information ~~is initiated if personal information is collected~~ from a source other than the applicant or public records.

2. In the case of a policy renewal, ~~a notice no later than the policy renewal date, except that no notice is required in connection with a policy renewal if personal information is collected only from the policyholder or from public records or a notice meeting the requirements of this section has been given within the previous twenty-four months~~ AT LEAST ANNUALLY DURING THE CONTINUATION OF THE RELATIONSHIP WITH THE POLICYHOLDER.

3. In the case of a policy reinstatement or change in insurance benefits, ~~a notice no~~ NOT later than the time WHEN THE INSURANCE INSTITUTION RECEIVES a request for a policy reinstatement or change in insurance benefits ~~is received by the insurance institution,~~ except that ~~no~~ A notice is NOT required if ~~personal information is collected only from the policyholder or from public records~~ A NOTICE WAS ALREADY GIVEN WITHIN THE IMMEDIATELY PRECEDING TWELVE MONTHS.

~~B.~~ C. The notice shall be in writing OR, IF THE APPLICANT OR POLICYHOLDER AGREES, IN AN ELECTRONIC FORM and SHALL EITHER CONTAIN THE INFORMATION REQUIRED FOR COMPLIANCE WITH THE NOTICE REQUIREMENTS ESTABLISHED UNDER SECTION 503 OF THE GRAMM LEACH BLILEY ACT (15 UNITED STATES CODE SECTION 6803) OR SHALL state:

1. Whether personal information may be collected from persons other than the individual or individuals proposed for coverage.

2. The types of personal information that may be collected and the types of sources and investigative techniques that may be used to collect ~~such~~ THE information.

3. The types of disclosures identified in section 20-2113, paragraphs 2 through 6, 9, 11, 12 and 14 and the circumstances under which the disclosures may be made without prior authorization, except only those circumstances need be described which occur with such a frequency as to indicate a general business practice.

4. A description of the rights established under sections 20-2108 and 20-2109 and the manner in which those rights may be exercised.

5. That information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

~~C.~~ D. Instead of the notice prescribed in subsection ~~B~~ C of this section, the insurance institution or agent may provide an abbreviated notice informing the applicant ~~or policyholder~~ that:

1. Personal information may be collected from persons other than the individual or individuals proposed for coverage.

2. The information as well as other personal or privileged information subsequently collected by the insurance institution or agent may in certain circumstances be disclosed to third parties without authorization.

3. A right of access and correction exists with respect to all personal information collected.

4. The notice prescribed in subsection ~~B~~ C of this section will be ~~furnished~~ PROVIDED to the applicant ~~or policyholder upon~~ ON request.

~~D.~~ E. The obligations imposed by this section ~~upon~~ ON an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf.

F. IF AN INSURANCE INSTITUTION, AGENT OR INSURANCE SUPPORT ORGANIZATION THAT IS REQUIRED TO GIVE NOTICE UNDER THIS SECTION GIVES THE NOTICE TO THE SPONSOR OF AN EMPLOYEE BENEFIT PLAN, A GROUP OR BLANKET INSURANCE POLICYHOLDER OR GROUP ANNUITY CONTRACT HOLDER OR A WORKERS' COMPENSATION PLAN PARTICIPANT AND DOES NOT DISCLOSE PERSONAL INFORMATION ABOUT ANY OF THE INDIVIDUALS DESCRIBED IN PARAGRAPH 1, 2 OR 3 OF THIS SUBSECTION EXCEPT AS OTHERWISE ALLOWED UNDER SECTION 20-2113, THE INSURER, PRODUCER OR INSURANCE SUPPORT ORGANIZATION IS NOT REQUIRED TO PROVIDE THE NOTICE TO:

1. A PARTICIPANT OR A BENEFICIARY OF AN EMPLOYEE BENEFIT PLAN THAT THE INSURER ADMINISTERS OR SPONSORS OR FOR WHICH THE INSURER ACTS AS TRUSTEE, INSURER OR FIDUCIARY.

2. AN INDIVIDUAL WHO IS COVERED UNDER A GROUP OR BLANKET INSURANCE POLICY OR GROUP ANNUITY CONTRACT ISSUED BY THE INSURER.

3. A BENEFICIARY IN A WORKERS' COMPENSATION PLAN.

G. AN INSURANCE INSTITUTION OR AGENT IS NOT REQUIRED TO GIVE NOTICE UNDER THIS SECTION TO A POLICYHOLDER WHOSE POLICY IS LAPSED, EXPIRED OR OTHERWISE INACTIVE IF THE INSURANCE INSTITUTION OR AGENT HAS NOT COMMUNICATED WITH THE POLICYHOLDER FOR AT LEAST TWELVE CONSECUTIVE MONTHS, OTHER THAN TO PROVIDE ANNUAL PRIVACY NOTICES, MATERIAL REQUIRED BY LAW OR ORDER OF A STATE OR FEDERAL REGULATORY AUTHORITY OR PROMOTIONAL MATERIALS.

H. AN INSURANCE INSTITUTION OR AGENT IS NOT REQUIRED TO GIVE NOTICE UNDER THIS SECTION TO A POLICYHOLDER WHOSE LAST KNOWN ADDRESS OF RECORD IS INVALID. AN ADDRESS IS DEEMED INVALID UNDER THIS SUBSECTION IF MAIL SENT TO THAT ADDRESS BY THE INSURANCE INSTITUTION OR AGENT HAS BEEN RETURNED BY THE POSTAL AUTHORITIES AS UNDELIVERABLE AND IF SUBSEQUENT ATTEMPTS BY THE INSURANCE INSTITUTION OR AGENT TO OBTAIN A VALID ADDRESS FOR THE INDIVIDUAL HAVE BEEN UNSUCCESSFUL.

Sec. 3. Section 20-2113, Arizona Revised Statutes, is amended to read:

20-2113. Disclosure limitations and conditions

An insurance institution, agent or insurance support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is:

1. With the written authorization of the individual except that:

(a) If the authorization is submitted by another insurance institution, agent or insurance support organization, the authorization ~~meets~~ SHALL MEET the ~~requirement of~~ REQUIREMENTS PRESCRIBED IN section 20-2106.

(b) If the authorization is submitted by a person other than an insurance institution, agent or insurance support organization, the authorization ~~is~~ SHALL BE dated, signed by the individual and obtained one year or less prior to the date a disclosure is sought pursuant to this ~~subsection~~ SECTION.

2. To a person other than an insurance institution, agent or insurance support organization, if the disclosure is reasonably necessary:

(a) To enable the person to perform a business, professional or insurance function for the disclosing insurance institution, agent or insurance support organization and the person agrees not to disclose the information further without the individual's written authorization unless the further disclosure either:

(i) Would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization.

(ii) Is reasonably necessary for the person to perform his function for the disclosing insurance institution, agent or insurance support organization.

(b) To enable the person to provide information to the disclosing insurance institution, agent or insurance support organization for the purpose of determining an individual's eligibility for an insurance benefit or payment or detecting or preventing criminal

activity, fraud, material misrepresentation or material nondisclosure in connection with an insurance transaction.

3. To an insurance institution, agent, insurance support organization or self-insurer if the information disclosed is limited to that which is reasonably necessary to detect or prevent criminal activity, fraud, material misrepresentation or material nondisclosure in connection with insurance transactions or for either the disclosing or receiving insurance institution, agent or insurance support organization to perform its function in connection with an insurance transaction involving the individual.

4. To a medical care institution or medical professional for the purpose of verifying insurance coverage or benefits, informing an individual of a medical problem of which the individual may not be aware or conducting an operations or service audit, if only the information which is reasonably necessary to accomplish the purposes prescribed by this paragraph is disclosed.

5. To an insurance regulatory authority.

6. To a law enforcement or other governmental authority to protect the interests of the insurance institution, agent or insurance support organization in preventing or prosecuting the perpetration of fraud upon it, or if the insurance institution, agent or insurance support organization reasonably believes that illegal activities have been conducted by the individual.

7. Otherwise permitted or required by law.

8. In response to a valid administrative or judicial order, including a search warrant or subpoena.

9. Made for the purpose of conducting actuarial or research studies, except that no individual may be identified in any actuarial or research report, materials allowing the individual to be identified ~~are~~ SHALL BE returned or destroyed as soon as they are no longer needed and the actuarial or research organization ~~agrees~~ SHALL AGREE not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization.

10. To a party or a representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the insurance institution, agent or insurance support organization, except that prior to the consummation of the sale, transfer, merger or consolidation only the information is disclosed which is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger or consolidation and the recipient agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization.

11. To a person whose only use of the information will be in connection with the marketing of a product or service if:

(a) No medical record information, privileged information or personal information relating to an individual's character, personal habits, mode of living or general reputation is disclosed and no classification derived from the information is disclosed.

(b) The individual has been given an opportunity to indicate that the individual does not want personal information disclosed for marketing purposes and has given no indication that the individual does not want the information disclosed.

(c) The person receiving the information agrees not to use it except in connection with the marketing of a product or service.

12. To an affiliate whose only use of the information will be in connection with an audit of the insurance institution or agent or the marketing of an insurance OR FINANCIAL product or service, if the affiliate agrees not to disclose the information for any other purpose or to an unaffiliated person, EXCEPT THAT NO MEDICAL RECORD INFORMATION MAY BE DISCLOSED FOR MARKETING PURPOSES WITHOUT THE INDIVIDUAL'S WRITTEN CONSENT.

13. By a consumer reporting agency if the disclosure is to a person other than an insurance institution or agent.

14. To a group insurance policyholder for the purpose of reporting claims experience or conducting an audit of the insurance institution's or agent's operations or services if the information disclosed is reasonably necessary for the recipient to conduct the review or audit.

15. To a professional peer review organization for the purpose of reviewing the service or conduct of a medical care institution or medical professional.

16. To a governmental authority for the purpose of determining the individual's eligibility for health benefits for which the governmental authority may be liable.

17. To a certificate holder or policyholder for the purpose of providing information regarding the status of an insurance transaction.

Sec. 4. Title 20, chapter 11, article 1, Arizona Revised Statutes, is amended by adding section 20-2121, to read:

20-2121. Enforcement of privacy provisions of Gramm Leach Bliley act

A. THE DEPARTMENT MAY ENFORCE TITLE V, SUBTITLE A OF THE GRAMM LEACH BLILEY ACT (15 UNITED STATES CODE SECTIONS 6801 THROUGH

6809) RELATED TO PRIVACY AND PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

B. THE DIRECTOR MAY ADOPT RULES PURSUANT TO TITLE 41, CHAPTER 6 TO CARRY OUT THIS SECTION.

State Regulation of Health Information: Arizona and Nevada

Exhibit 5

Gramm-Leach-Bliley Act Implementation

- **Nevada Bill AB 618 (Excerpt)**
- **Nevada Financial Privacy Proposed Temporary Regulation R113-00P (Cause No. 00-167)**

Nevada
Assembly Bill No. 618–Committee on Commerce and Labor

CHAPTER.....

AN ACT relating to insurance; providing for the regulation of the business of viatical settlements; requiring the commissioner of insurance to adopt regulations governing the use of electronic records and signatures; temporarily authorizing the adoption of regulations to enforce federal law concerning a bill of rights for patients; limiting the disclosure of certain information concerning consumers; providing for the conversion of domestic mutual insurers into domestic stock insurers; providing for the reorganization of domestic mutual insurers into mutual insurance holding companies; making various other changes concerning the regulation of insurance; providing penalties; and providing other matters properly relating thereto.

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

****

Sec. 135. Chapter 686A of NRS is hereby amended by adding thereto a new section to read as follows:

1. Disclosure of nonpublic personal information in a manner contrary to the provisions of subchapter 1 of Title V of Public Law 106-102, 15 U.S.C. §§ 6801-6809 is an unfair act or practice in the business of insurance within the meaning of this chapter.

2. As used in this section "nonpublic personal information" has the meaning ascribed to it in 15 U.S.C. § 6809(4).

3. The commissioner shall adopt regulations necessary to carry out the provisions of this section.

STATE OF NEVADA
DEPARTMENT OF BUSINESS AND INDUSTRY
DIVISION OF INSURANCE

FINANCIAL PRIVACY
PROPOSED TEMPORARY REGULATION

AUTHORITY: NRS 679b.130; NRS 233b.040; title V of the Gramm-Leach-Bliley Act (U.S.C. 6801 through 6827)

Section 1. "Licensees" means all insurers, agents, brokers, other persons licensed or required to be licensed or authority pursuant to Title 57 of the Nevada Revised Statutes.

Sec. 2 In order to provide sufficient time for licensees to establish policies and procedures to comply with the requirements under Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 through 6827) which becomes effective November 13, 2000, the Commission has extended the time for licensees for compliance with Title V to July 1, 2001.

Sec. 3 The provisions of section 2 become effective on November 13, 2000.