Arizona Health-e Connection Legal Working Group

Development of a Framework for Privacy, Security, and Accountability in HIE
Existing Federal and Arizona Laws

FEDERAL HEALTH-RELATED LAWS

Citation	Summary
HIPPA	
Privacy Rule, 45 CFR Part 160, Part 164, Subpart E	Detailed requirements regarding appropriate internal use and external disclosure of protected health information.
Security Rule, 45 CFR Part 160, Part 164, Subpart C	Detailed requirements regarding the administrative, technical, and physical security procedures required to protect electronic protected health information.
42 USC 1176	Civil penalties: not more than $100 for each violation, up to a total of $25,000 for all violations of an identical requirement or prohibition during a calendar year.
42 USC 1177	Criminal penalties: "A person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person" may: "(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both."
Enforcement Rule, 45 CFR Part 160, Subpart C	Procedural rules for enforcement of civil penalties.
Substance Abuse Treatment Regulations	
42 CFR Part 2	Detailed requirements regarding the use and disclosure of information by a federally-assisted drug or alcohol abuse treatment program.
42 USC 290ee-3(f), 42 USC 290dd-3(f), 42 CFR 2.4, 42 CFR 2.5	Criminal penalties: Not more than $500 for a first offense; not more than $5,000 for each subsequent offense.

Medicare Conditions of Participation	
42 CFR § 482.13 Patient Rights COP	42 CFR § 482.13(c)(1) (patient right to personal privacy); 42 CFR § 482(d)(1) (patient right to confidentiality of clinical records).
42 CFR § 482.24 Medical Records COP	42 CFR § 482.24(b) (requiring system of author identification and record maintenance to ensure the integrity of the authentication and protects the security of all record entries); 42 CFR § 482.24(b)(3) (requiring procedure for ensuring the confidentiality of patient records).
The Genetic Information Nondiscrimination Act of 2008	
General Pub. L. No. 110-233, 122 Stat. 881	Prohibits discrimination in health insurance and employment on the basis of genetic information. Genetic information is defined as information about (a) an individual's genetic tests, (b) the genetic tests of family members of the individual, and (c) the manifestation of a disease or disorder in family members of the individual.
Health Insurance	• Prohibits health insurance insurers from raising premiums or denying coverage on the basis of genetic information. • Does not, however, limit the ability of a health insurance insurer to increase premiums based on the manifestation of a disease or disorder in an enrolled individual. • Revises the HIPAA privacy regulations to clarify that genetic information must be treated as health information.
Employment	• Makes it unlawful for employers to use genetic information for decisions regarding hiring, discharging, or classifying employees. • Prohibits employers from otherwise discriminating against employees regarding compensation, terms, conditions, and privileges of employment on the basis of genetic information. • Requires employers who possess genetic information about an employee to maintain the information on separate forms and in separate medical files and to treat the information as a confidential medical record of the employee.

FEDERAL COMPUTER-RELATED LAWS

Citation	Summary
18 U.S.C. § 1028 Identity Theft	Punishes A person who knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document that is or appears to be issued by or under the authority of the United States or the production, transfer, possession, or use is in or that affects interstate or foreign commerce, including the transfer of a document by electronic means. Penalties: A fine or imprisonment of up to 30 years (depending on the circumstances), or both.
18 U.S.C. § 1030 Computer Fraud	Punishes fraud and related activity in connection with computer, for anyone who: • Intentionally accesses a computer **without authorization** or **exceeds authorized access** and obtains information from any **protected computer** if the conduct involved an interstate or foreign communication. 18 U.S.C. § 1030(a)(2)(C). The term **'protected computer'** means a computer which is used in interstate commerce or communication. 18 U.S.C. § 1030e)(2)(A). • Knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and furthers the intended fraud and obtains anything of value. 18 U.S.C. § 1030(a)(4).

	• Knowingly causes the transmission of a program, information, code, or command, and as a result, intentionally causes **damage** without authorization, to a protected computer. 18 U.S.C. § 1030 (a)(5)(A)(i). The term '**damage**' means any impairment to the integrity or availability of data, a program, a system, or information. 18 U.S.C. § 1030 (e)(8). Penalties: A fine or imprisonment of up to 20 years. (depending on the circumstances), or both.

ARIZONA HEALTH-RELATED LAWS

Citation	Summary
A.R.S. § 12-2291, *et seq.* Medical Records Laws	Confidentiality: Makes all medical records and payment records, and the information contained in medical records and payment records, privileged and confidential. • Permits health care provider to disclose only that part or all of a patient's medical records and payment records as are authorized by state or federal law or written authorization signed by the patient or the patient's health care decision maker. • Permits health care providers to follow the HIPAA Privacy Rule in how they use or disclose health information. • Lists the types of disclosures health care providers may make without getting patient authorization. Enforcement: No enforcement agency or penalties for violation specified. Immunity: Immunity for good faith compliance: A.R.S. § 12-2296 ("A health care provider or contractor that acts in good faith under this article is not liable for damages in any civil action for the disclosure of medical records or payment records or information contained in medical records or payment records that is made pursuant to this article or as otherwise provided by law. The health care provider or contractor is presumed to have acted in good faith. The presumption may be rebutted by clear and convincing evidence."
A.R.S. § 12-2801, *et seq*. Genetic Testing Information	Confidentiality: The results of a genetic test are confidential and may be released only to individuals expressly listed in the statute. When a person has received genetic testing information from someone else, that recipient also must follow the state statutory rules on disclosing that information. Information and records held by a state agency or a local health authority relating to genetic testing information are confidential and are exempt from public copying and inspection. (Note that under A.R.S. § 20-448.02, health plans are subject to even more restrictive rules on disclosing genetic testing information, and may not release those results to any party without the written, express consent of the subject of the test.) Enforcement: No enforcement agency or penalties for violation specified. Immunity: Immunity for good faith compliance: A.R.S. § 12-2802(G) ("A health care provider and the provider's agents and employees that act in good faith and that comply with this article are not subject to civil liability. The good faith of a health care provider that complies with this article is presumed. The presumption may be rebutted by a preponderance of the evidence.")

A.R.S. § 36-135 and A.A.C. R9-6-708 Immunization Information	Confidentiality: Identifying information in the system is confidential. A person who is authorized to receive confidential information under these statutes shall not disclose this information to any other person. A.R.S. § 36-135(E). Enforcement: A health care professional who does not comply with these requirements violates a law or task applicable to the practice of medicine and an act of unprofessional conduct. A.R.S. § 36-135(G). Any agency or person receiving confidential information from the system who subsequently discloses that information to any other person is guilty of a class 3 misdemeanor. A.R.S. § 36-135(H). Immunity: A health care professional who provides information in good faith pursuant to this section is not subject to civil or criminal liability. A.R.S. § 36-135(F).
A.R.S. § 36-501, *et seq*. Mental Health Information	Confidentiality: Mental health providers and health care institutions licensed as behavioral health providers must keep mental health records, and the information contained in mental health records, confidential. A.R.S. § 36-509. These providers may disclose mental health information only as expressly permitted by the statute. • Mental health providers are physicians and other providers of mental health or behavioral health services that are involved in evaluating, caring for, treating or rehabilitating a patient. A.R.S. § 36-501(27). • Health care institutions licensed as behavioral health providers include hospitals with behavioral health licenses for inpatient psychiatric units and outpatient clinics providing behavioral health services. • Other health care providers that provide mental or behavioral health services (such as a hospital emergency department that provides psychiatric consultations) are not subject to the confidentiality provisions in the Arizona mental health statutes and regulations. Enforcement: Any knowing violation of a person's rights under these statutes shall give him a cause of action for the greater of either one thousand dollars or three times the actual amount of damages. It is not a prerequisite to this action that the plaintiff suffers or be threatened with actual damages. A.R.S. § 36-516. Immunity: An agency or nonagency treating professional that makes a decision to release or withhold treatment information in good faith pursuant to these statutes is not subject to civil liability for this decision. A.R.S. § 36-517.01(C).
A.R.S. § 36-661 *et seq*., Communicable Disease Information	Confidentiality: • A person who obtains communicable disease related information in the course of providing a health service or obtains that information from a health care provider pursuant to an authorization and a person to whom communicable disease related information is disclosed pursuant to this statute shall not disclose the information to another person except as authorized in the statute. A.R.S. § 36-664. • Separate provisions govern when a state, county or local health department or officer may disclose communicable disease related information. A.R.S. § 36-664(C). • Additional restrictions in the Insurance Code apply to health plans' release of HIV/AIDS information. A.R.S. § 20-448.01. An insurer's disclosure of HIV-related information must be accompanied by a written statement that warns that the information is protected by state law that prohibits further disclosure of the information without the specific written consent of the person to whom it pertains or as otherwise permitted by law.

	Enforcement: • A person who knowingly: (1) performs, or permits or procures the performance of, an HIV-related test in violation of this statute; or (2) discloses, compels another person to disclose or procures the disclosure of communicable disease related information in violation of this statute is guilty of a class 3 misdemeanor. A.R.S. § 36-666. • ADHS may impose a civil penalty of not more than five thousand dolalrs if a person (1) performs, or permits or procures the performance of, an HIV-related test in violation of this statute; or (2) discloses, compels another person to disclose or procures the disclosure of communicable disease related information in violation of this statute. A.R.S. § 36-667. • A protected person may bring an action in superior court for legal and equitable relief on his own behalf against a person who violates this article. A.R.S. § 36-668. Immunity: • A person, health facility, or health care provider disclosing communicable disease related information pursuant to or required by this statute is immune from civil or criminal liability if the person, health care facility or health care provider acted in good faith and without malice. A.R.S. § 36-666(B). • A health facility or health care provider, including a physician, the physician's employer or the health care facility or health care provider with which the physician is associated, is immune from civil or criminal liability for failing to disclose communicable disease related information to a contact or a person authorized pursuant to law to consent to health care for a protected person if the health facility or health care provider acted in good faith and without malice. A.R.S. § 36-666(C). • Good faith and the absence of malice are presumed unless the presumption is overcome by a demonstration of clear and convincing evidence to the contrary. A.R.S. § 36-666(D).
Arizona Department of Health Services	Confidentiality: See provisions for specific types of health care institutions below. Enforcement: A.R.S. § 36-427(A): The director may suspend or revoke, in whole or in part, the license of any health care institution if its owners, officers, agents or employees: 1. Violate this chapter or the rules of the department adopted pursuant to this chapter. 2. Knowingly aid, permit or abet the commission of any crime involving medical and health related services. 3. Have been, are or may continue to be in substantial violation of the requirements for licensure of the institution, as a result of which the health or safety of one or more patients or the general public is in immediate danger. A.R.S. § 36-431.01(A). The director may assess a civil penalty against a person who violates this chapter or a rule adopted pursuant to this chapter in an amount of not to exceed five hundred dollars for each violation. Each day that a violation occurs constitutes a separate violation. A.A.C. R9-10-110: If a licensed health care institution is not in substantial compliance with applicable laws and rules, the Department may: 1. Issue a provisional license under A.R.S. § 36-425; 2. Assess a civil penalty under A.R.S. § 36-431.01;

	3. Impose an intermediate sanction under A.R.S. § 36-427; 4. Remove a licensee and appoint another person to continue operation of the health care institution pending further action under A.R.S. § 36-429; 5. Suspend or revoke a license under A.A.C. R9-10-111 and A.R.S. § 36-427; 6. Deny a license under A.A.C. R9-10-111; or 7. Issue an injunction under A.R.S. § 36-430. **A. HOSPITALS** A.A.C. R9-10-209(A)(6). Hospital medical record information may be disclosed only with the written consent of a patient or the patient's representative or as permitted by law. A.A.C. R9-10-228(A)(6). Information in a hospital medical record may be disclosed to personnel members, medical staff members authorized by hospital policies and procedures to access the medical record, as authorized by the written consent of a patient or the patient's representative, or as permitted by law. A.A.C. R9-10-228(A)(10). A hospital medical record must be protected from unauthorized use. **B. ADULT DAY HEALTH CARE FACILITIES** A.A.C. R9-10-505(E)(5). A participant shall have the right to have medical and financial records kept in confidence. The release of such records shall be by written consent of the participant or participant's representative, except as otherwise required or permitted by law. A.A.C. R9-10-511(C). Records shall be protected at all times from unauthorized use. **C. ASSISTED LIVING FACILITIES** A.A.C. R9-10-703(B)(1)(f). A licensee shall ensure that a manager of an assisted living facility develops and implements written policies and procedures for the day-to-day operation of the assisted living facility including protecting and releasing resident records and maintaining confidentiality of resident records. A.A.C. R9-10-710(D)(12). A licensee shall ensure that a resident has the right to have financial and other records kept in confidence. The release of records shall be by written consent of the resident or the representative, except as otherwise provided by law. A.A.C. R9-10-714(B)(1). A licensee shall ensure that a resident's record is confidential and only released with written permission from the resident or the representative, or as otherwise provided by law. **D. HOSPICES** A.A.C. R9-10-812(2) & 814(B)(4). A hospice licensee shall Maintain confidentiality of patient records, as required in A.R.S. Title 12, Chapter 13, Article 7. **E. NURSING CARE INSTITUTIONS** A.A.C. R9-10-913(A). An administrator shall ensure that: (5) Information in a medical record is disclosed only with the written

	consent of a resident or the resident's representative or as permitted by law. (8)(a) A medical record is protected from loss, damage or unauthorized use. A.A.C. R9-10-913(B)(1). If a nursing care institution keeps medical records electronically, an administrator shall ensure that Safeguards exist to prevent unauthorized access. **F. HOME HEALTH AGENCIES** A.A.C. R9-10-1107(C)(6). Personnel shall ensure that language barriers or physical handicaps do not prevent each patient or patient's representative from becoming aware of the patient's right to have financial and medical records kept in confidence. The release of such records shall be by written consent of the patient or patient's representative, except as otherwise required or permitted by law. A.A.C. R9-10-1108(A). The administrator shall ensure the maintenance of policies and procedures governing the protection and confidentiality of medical records. **G. RECOVERY CARE CENTERS** A.A.C. R9-10-1403(D)(4). Each patient shall have the right to have medical and financial records kept in confidence. The release of such records shall be by written consent of the patient or the patient's representative except as otherwise required or permitted by law. **H. ABORTION CLINICS** A.A.C. R9-10-1503(C)(5). A medical director shall ensure written policies and procedures are developed and implemented for accessibility and security of patient medical records. A.A.C. R9-10-1507(3). A licensee shall ensure that a patient is afforded the rights and is informed of the right to have medical records kept confidential. A.A.C. R9-10-1511(A), A licensee shall ensure that: (1) A medical record is accessible only to the Department or personnel authorized by the abortion clinic's policies and procedures. (2) Medical record information is confidential and released only with the written informed consent of a patient or the patient's representative or as otherwise permitted by law. (3) A medical record is protected from unauthorized use. **I. OUTPATIENT SURGICAL CENTERS** A.A.C. R9-10-1710(C). Staff shall release medical record information only after receiving the patient's or patient representative's written consent, or as otherwise required or permitted by law.
Nursing Care Institution Administrators and Assisted Living Facilities Managers	Confidentiality/Enforcement: A.R.S. § 36-446.07 (A)(7) The board may suspend or revoke the license of any nursing care institution administrator, censure or place on probation any licensed nursing care institution administrator or deny a license as a nursing care institution administrator to any person for the unauthorized disclosure of information relating to a patient or

	a patient's records. (B)(7) The board may suspend or revoke the certificate of an assisted living facility manager, censure or place on probation an assisted living facility manager or deny a certificate as an assisted living facility manager to a person for the unauthorized disclosure of information relating to a resident or a resident's records. (C) The board may impose a civil penalty in an amount of not to exceed five hundred dollars on any nursing care institution administrator or assisted living facility manager who violates this article or any rule adopted pursuant to this article.
Professional Licensing Boards	Confidentiality: A.R.S. § 32-3211. A health professional must prepare a written protocol for the secure storage, transfer and access of the medical records of the health professional's patients. The protocol must comply with the relevant requirements A.R.S. § 12-2291, *et seq*. described above. See provisions below for statutes relating to each professional licensing board. Enforcement: • A health professional who does not comply with this statute commits an act of unprofessional conduct and is subject to discipline by the applicable regulatory board. A.R.S. § 32-3211. • In addition, the health professional's regulatory board may take corrective action regarding the proper storage, transfer and access of the medical records of the health professional's patients. A.R.S. § 32-3211. • See provisions below for statutes relating to each professional licensing board. These enforcement statutes allow licensing boards to take a variety of enforcement actions, which generally include the ability to: o Restrict a license or order a summary suspension of a license pending proceedings for revocation or other action. o Require the licensee to complete designated continuing education courses. o File an advisory letter. o Enter into a consent agreement to limit or restrict the professional's practice or to rehabilitate the professional. o Require the professional to successfully complete a board approved rehabilitative, retraining or assessment program. o Revoke or suspend a license. o File a letter of reprimand. o Issue a decree of censure. o Fix a period and terms of probation best adapted to protect the public health and safety and rehabilitate or educate the professional. o Impose a civil penalty.
	Arizona Medical Board Confidentiality: "Unprofessional conduct" includes violating any federal of state laws, rules or regulations applicable to the practice of medicine and intentionally disclosing a privileged communication. A.R.S. § 32-1401(27)(a), (b) and (e). Enforcement: A.R.S. §32-1451.

	Board of Osteopathy Confidentiality: A.R.S. § 32-1854. Unprofessional conduct includes: (1) Willfully violating a privileged communication. (19) Any conduct or practice contrary to recognized standards of ethics of the osteopathic medical profession. (35) Violating a federal law, a state law or a rule applicable to the practice of medicine. Enforcement: A.R.S. § 32-1855(I).
	Board of Nursing Confidentiality: A.R.S. §32-1601 (16)(g). "Unprofessional conduct" includes willfully or repeatedly violating a provision of this chapter or a rule adopted pursuant to this chapter. A.A.C. R4-19-814(B)(10) – Applicable to CNAs. For the purposes of A.R.S 32-1601(16), a practice that is harmful is violating a patient right of privacy by disclosing confidential information or knowledge concerning the patient. A.A.C. R-4-19-403 (16) – Applicable to LPNs. Unprofessional conduct includes removing, without authorization, a medical record from any health care facility, school, institution, or other work place location. Enforcement: A.R.S. § 32-1663(D).
	Board of Respiratory Care Confidentiality: A.R.S. § 32-3501(10). "Unprofessional Conduct" includes (i) any conduct that is contrary to recognized standards of ethics of the respiratory therapy profession. A.A.C. R4-45-214(14). Standards of ethics for the respiratory care profession include not violating the confidentiality of information concerning a patient. Enforcement: A.R.S. § 32-3553.
	Board of Physical Therapy Confidentiality: A.R.S. § 32-2044(19). Licensed Physical Therapists who fail to maintain patient confidentiality without prior written consent of the patient are grounds for disciplinary action by the Board. A.A.C. R4-24-301(B). A physical therapist shall maintain the confidentiality of patient records in accordance with the Arizona Medical Record Laws. A.R.S. § 32-2051(f). Information relating to the physical therapist-patient relationship is confidential and shall not be communicated to a third party who is not involved in that patient's care without the prior written consent of the patient. Enforcement: A.R.S. § 32-2047.

	Podiatry Board Confidentiality: A.R.S. § 32-852(A). The Board may suspend, revoke or refuse to issue a license upon proof that the licensee willfully revealed a privileged communication except as required by law or if the licensee is guilty of unprofessional conduct. A.R.S. § 32-854.01 (18). "Unprofessional conduct" included violating any federal or state law applicable to the practice of podiatry. Enforcement: A.R.S. § 32-852.01.
	Chiropractic Board Confidentiality: A.A.C. R4-7-902(13). "Unprofessional conduct" includes violating any federal or state law or rule or regulations applicable to the practice of chiropractic care. Enforcement: A.R.S. § 32-924 (B)-(L).
	Dentistry Board Confidentiality: A.R.S. § 32-1201(20)(a). "Unprofessional conduct" means the intentional betrayal of a professional confidence or intentional violation of a privileged communication. Enforcement: A.R.S. § 32-1263.01.
	Naturopathy Board Confidentiality: A.R.S. § 32-1501. "Unprofessional conduct" includes: (a) intentionally disclosing a professional secret or intentionally disclosing a privileged communication. Enforcement: A.R.S. § 32-1551.
	Dispensing Opticians Confidentiality: A.R.S. § 32-1696(A)(8). It is unlawful for a dispensing optician to fraudulently, dishonestly, illegally or unprofessionally conduct the practice of optical dispensing. See also A.A.C. R4-20-118. Enforcement: A.R.S. § 32-1693.

	Optometry Board Confidentiality: A.R.S. § 32-1701(a). "Unprofessional conduct" includes willful betrayal of a professional secret or willful violation of a privileged communication. A.R.S. § 32-1746(B). All patient records are confidential and are not public records. Enforcement: A.R.S. § 32-1743(4) and (10).
	Pharmacy Confidentiality: A.R.S. § 32-1964(D). A pharmacist, pharmacy permittee or pharmacist in charge shall comply with applicable state and federal privacy statutes and regulations when releasing patient prescription information. A.A.C. R4-23-404(F). A pharmacist must maintain confidentiality of patient records to ensure that computer records system has security and safeguards systems. Enforcement: A.R.S. § 32-1904(B)(8).
	Psychology Confidentiality: A.R.S. § 32-2085. The confidential relations and communication between a client and a psychologist are privileged. The psychologist shall ensure that client records and communications are treated by clerical and paraprofessional staff at the same level of confidentiality and privilege required by the psychologist. A.A.C. R4-26-101(11). "Confidential record" means a record that is classified as confidential by statute. A.A.C. R4-26-101(9). "Client Record" means medical records as defined in the [the medical records statute] A.R.S. § 12-2291(5). A.A.C. R4-26-106(B). Without a client's consent, a psychologist shall release a client's raw test data or psychometric testing materials only to the extent required by federal or Arizona law or court order compelling production. A.R.S. § 32-2061(13). "Unprofessional conduct" includes: (b) betraying professional confidences, (r) failing to obtain a client's informed and written consent to release personal or otherwise confidential information to another party unless the release is otherwise authorized by law. Enforcement: A.R.S. § 32-2081.

	Physician Assistants Confidentiality: A.R.S. § 32-2501(21)(ee). "Unprofessional conduct" includes intentionally betraying a professional secret or intentionally violating a privileged communication. Enforcement: A.R.S. § 32-2551.
	Radiologic Technologists Confidentiality: A.R.S. § 32-2801(17)(a). "Unethical professional conduct" means the intentional betrayal of a professional confidence or intentional violation of a privileged communication. Enforcement: A.R.S. § 32-2821(A)(7).
	Homeopathic Physicians Confidentiality: A.R.S. § 32-2933. "Unprofessional conduct" includes: (2) willful betrayal of a professional secret or willful violation of a privileged communication and (5) violation of federal, state county or municipal laws or regulations applicable to the practice of medicine or relating to public health. Enforcement: A.R.S. § 32-2934.
	Behavioral Health Professionals Confidentiality: A.A.C. R4-6-1105(A). A licensee shall only release or disclose client records or any information regarding a client: (1) in accordance with applicable federal or state law that authorizes release or disclosure; or (2) with written authorization from the client or the client's legal representative. A.R.S. § 32-3251. "Unprofessional conduct" includes: (t) disclosing a professional confidence or privileged communication, (gg) failing to follow federal and state laws regarding the storage, use and release of confidential information regarding a client's personal identifiable information and care. A.A.C. R4-6-1103(A)(2). A licensee must ensure that a client record is kept confidential. A.R.S. § 32-3283(A). The confidential relationship between a client and a licensee is privileged. A licensee shall not voluntarily or involuntarily divulge information that is received by reason of the confidential nature of the behavioral health professional-client relationship. A.A.C. R4-6-1001(2)(C). Behavioral health professionals must explain to clients that the client has a right to have client records and that all information regarding the client be kept confidential and be explained the limitations on confidentiality. Enforcement: 3 A.R.S. § 2-3281.

	Occupational Therapy Confidentiality: A.R.S. § 32-3401(h). "Unprofessional conduct" includes any conduct or practice contrary to recognized standards of ethics of occupational therapy profession Enforcement: A.R.S. § 32-3442.
	Acupuncture Confidentiality: A.R.S. § 32-3901. "Unprofessional conduct" includes (a) willfully disclosing a professional secret or willfully violating a privileged communication, (l) conduct that is contrary to the recognized standards or ethics of the acupuncture profession Enforcement: A.R.S. § 32-3951.

ARIZONA COMPUTER-RELATED LAWS

Citation	Summary
A.R.S. § 13-2008 Identify Theft	A person commits taking the identity of another person if the person knowingly takes, purchases records, possesses, or uses any personal identifying information of another person, without the consent of that other person with the intent to obtain or use the other person's identity for any unlawful purpose or to cause loss to a person whether or not the person actually suffers any economic loss as a result of the offense. A.R.S. § 13-2008 (A) Violation of the section is a class 4 felony. A.R.S. § 13-2008 (E)
A.R.S. § 13-2009 Aggravated Identity Theft	A person commits aggravated identity theft when it involves identity theft of five or more individuals or entities. A.R.S. § 13-2009 Violation of the section is a class 3 felony. Id.
A.R.S. § 13-2010 Trafficking	A person commits trafficking in the identity of another person if the person knowingly sells, transfers or transmits any personal identifying information without the consent of the other person for any unlawful purpose or to cause the loss to the person whether or not the other person or entity actually suffers any economic loss. A.R.S. § 13-2010(A) Violation of this section is a class 2 felony. A.R.S. § 13-2010(C)
A.R.S. § 13-2316 Computer Tampering	A person who acts without authority or who exceeds authorization of use commits tampering by Knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by a medical institution. A.R.S. § 13-2316 (A)(7) Violation of this section is a class 6 felony. A.R.S. § 13-2316 (E)
A.R.S. § 13-2316.01 Access Device	A person commits unlawful possession of an access device by knowingly possessing or controlling an access device without the consent of the owner or authorized user and with the intent to use or distribute that access device. A.R.S. § 13-2316.01(A). "Access device" means any account number personal identification number, password, encryption key, biometric identifier or other means of account

	access that can be used to obtain access. A.R.S. § 13-2301(E)(2) Unlawful possession of one hundred or more access devices is a class 4 felony. Unlawful possession of five or more but fewer than one hundred access devices is a class 5 felony. Unlawful possession of fewer than five access devices is a class 6 felony. A.R.S. § 13-2316(C)
A.R.S. § 13-2316.02 Unauthorized release of confidential computer security information	A person commits unauthorized release of proprietary or confidential computer security information by communicating, releasing or publishing proprietary or confidential computer security information relating to a particular computer, computer system or network without the authorization of its owner or operator. A.R.S. § 13-2316.02 (A) Violation of this section is a class 6 felony. A.R.S. § 13-2316.02(D)
A.R.S. § 44-7501 Security Breach Reporting	Requires an owner or licensor of **unencrypted computerized data** that includes **personal information** that becomes aware of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, to conduct a reasonable investigation to promptly determine if there has been a breach of the security system. A breach in the security system, requires notice to the individuals affected (in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system). Notice is required by: 1. Written notice. 2. Electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act (P.L. 106-229; 114 Stat. 464; 15 United States Code section 7001). 3. Telephonic notice. 4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed fifty thousand dollars or that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following: (a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice. (b) Conspicuous posting of the notice on the web site of the person if the person maintains one. (c) Notification to major statewide media. <u>Enforcement</u>: The attorney general may bring an action to obtain actual damages for a willful and knowing violation of this section and a civil penalty not to exceed ten thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. <u>Exceptions</u>: 1. A person subject to the Gramm-Leach-Bliley Act; and 2. HIPAA covered entities. <u>Definitions</u>: 1. "Breach" "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and

	access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further willful unauthorized disclosure. 2. "Encrypted" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. 3. "Individual" means a person that is a resident of this state as determined by a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach. 4. "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency or any other legal or commercial entity. Person does not include the department of public safety, a county sheriff's department, a municipal police department, a prosecution agency or a court. 5. "Personal information:" (a) Means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable: (i) The individual's social security number. (ii) The individual's number on a driver license issued pursuant to A.R.S. § 28-3166 or number on a nonoperating identification license issued pursuant to A.R.S. § 28-3165. (iii) The individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account. (b) Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. 6. "Redact" means alter or truncate data such that no more than the last four digits of a social security number, driver license number, nonoperating identification license number, financial account number or credit or debit card number is accessible as part of the personal information.