STATE of ARIZONA – Government Information Technology Budget Unit

Statewide **I**nformation **S**ecurity and **P**rivacy **O**ffice	**SISPO STANDARD**	**TITLE: Data Breach Notification**
	P900-S910	**Effective Date: May 31, 2011**

1. AUTHORITY

Under the authority of A.R.S. § 41-3507 and Executive Order 2008-10, the Statewide Information Security and Privacy Office (SISPO) is responsible for ensuring development and implementation of risk mitigation strategies by each budget unit to identify threats and vulnerabilities to the confidentiality, integrity and availability of state information and the information technology infrastructure.

2. PURPOSE

This Standard identifies the minimum standards a budget unit shall implement and maintain to provide for the prompt identification, reporting, management and notification of a data breach related to an information security incident as defined by the GITA SISPO Information Security Incident Management Policy, P900.

3. SCOPE

This standard applies to all budget units whose workforce or contractors are authorized to access or use the state information infrastructure or who access, use or disclose state information at any location where such activity is performed. State information includes any format on any media (e.g. electronic, hardcopy, other records as defined by A.R.S. § 41-1350) including information conveyed by an oral communication.

4. STANDARD

4.1 DEFINITIONS

4.1.1 "AZNet" means the contractor for the State of Arizona telecommunications and network.

4.1.2 "Budget unit" means a department, commission, board, institution or other budget unit of the state organization receiving, expending, or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

4.1.3 "Chief Executive Officer" (CEO) means the chief executive officer of a budget unit (See also GITA Administrative Rule. R2-18-101(2)).

4.1.4 "Confidential Information" (CI) means information other than Restricted Personal Identifying Information (RPII) that may only be disclosed as permitted or required by state or federal law or administrative rule. Confidential information includes critical business infrastructure information as defined by ARS 41-1801 and critical infrastructure information as defined by the U.S. Department of Homeland Security (6 USC 131; 49 CFR 1520).

4.1.5 "Contractor" means an individual, government entity or non-government business entity providing products or services for a budget unit or on behalf of a budget unit. The term "contractor" includes a "business associate" as defined by HIPAA at 45 CFR 160-103 [insert hyperlink], temporary personnel or other third parties, including subcontractors or other agents utilized by a contractor, that are not part of the budget unit workforce but have access Restricted Personal Identifying Information (RPII), confidential or sensitive information or to the state information technology infrastructure.

4.1.6 "Data Breach" means an information security incident involving (1) unauthorized access of Restricted Personal Identifying Information (RPII) and (2) the unauthorized access poses a substantial risk of financial, reputational or other harm to individuals affected by the incident. (See the Notification of Breach of Security System, the Arizona data breach notification law, ARS 44-7501 and the Health Insurance Portability and Accountability Act (HIPAA) data breach notification standard, 45 CFR Part 164, Subpart D).

4.1.7 "Discovery" means the date and/or time a budget unitor contractor becomes aware of or reasonably believes an information security incident has occurred.

4.1.8 "Information Privacy Incident" means an information security incident resulting in unauthorized access of personal identifying information defined by this policy as Restricted Personal Identifiable Information (RPII), Confidential Information (CI) or Sensitive Information (SI).

4.1.9 "Information Security Incident" or "Incident" means an event, as referenced in ARS 41-3507(E), that a budget unit, a budget unit's or contractor, or the state reasonably believes has the potential to compromise the confidentiality, integrity, or availability of a RPII, CI or SI or the state information technology infrastructure.

4.1.10 "Restricted Personal Identifying Information" (RPII) means data elements that are a subset of confidential information and create a high severity risk information security incident from unauthorized access. The RPII also may be subject to the Arizona data breach notification law (ARS 44-7501) or HIPAA data

breach notification standard (45 CFR Part 164, Subpart D). The data elements defined as RPII by this policy are:

(a) An individual's first name or first initial and last name in combination with any one or more of the following data elements for the individual, when the data element is not encrypted, redacted or secured by any other method rendering the information unreadable, unusable or undecipherable:

- Social security number
- Driver license number
- Non-operating identification license number
- Financial account number, credit card number, debit card number, or charge card account number
- Financial account number, credit, debit, or charge card account number in combination with computer access information as defined by ARS 13-2301(E)(2), including any security code, access code, biometric identifier or record, password or user ID for access to any electronic file or account

(b) "Protected Health Information" (PHI) as defined by the Privacy Rule of the Health Insurance Portability and Accountability Act or 19961 (HIPAA) as maintained by a budget unit that must comply with HIPAA.[i]

4.1.11 "Sensitive Information" (SI) means personal identifying information or other categories of information that if disclosed are reasonably likely to adversely affect the best interest of the state or the best interest of an individual. SI may include personal identifying information as discussed in the Arizona statute Government Anti-Identification Procedures (ARS 41-4171 and 41-4172) when such information is not otherwise defined as "restricted personal identifying information" or "confidential information.

4.1.12 "Unauthorized Access" means to access, acquire, use, disclose, view, exchange, transmit, maintain, retain, modify, store, record, dispose of or destroy RPII, CI or SI without authority, in excess of authority or with the intent to compromise the confidentiality of the information. Unauthorized Access includes the loss or other unauthorized access of a device, technology component or record containing RPII, CI or SI or the destruction/disposal of records that does not comply with the Arizona Record Destruction law, ARS 44-7601.

4.2 DATA BREACH IDENTIFICATION AND RESPONSE BY WORKFORCE

4.2.1. A budget unit's information security incident management framework will include a documented process for identifying when an information security incident creates a risk of a data breach because of unauthorized access to Restricted Personal Indentifying Information (RPII).

4.2.2. Workforce shall be trained at minimum on what information is RPII, how to safeguard that information and who to notify if an information security incident involves unauthorized access of RPII. Workforce training should also include Confidential Information (CI) and/or Sensitive Information (SI) safeguards and incident reporting when the role of the workforce involves access, use or disclosure of this information. Training outcomes will be measured by success of workforce to understand their role to identify report or respond to an information security incident that is a data breach. The training requirements shall be consistent with the SISPO Information Security Incident Management Policy, P900.

4.2.3. An information security incident that is reasonably likely to result in a data breach shall be classified as a "high" risk event and submitted to the SISPO incident reporting and response system (IRR), consistent with SISPO Incident Submission and Response Standard P900-905.

4.2.4. The budget unit will collaborate with SISPO from the date of discovery to closure of an incident that involves a data breach.

4.2.5. When a data breach involves multiple budget units, the budget units involved will collaborate with system and other involved budget units (see SISPO Incident Submission and Response Standard, P900-S905, section 4.9).

4.3 DATA BREACH IDENTIFICATION AND RESPONSE BY CONTRACTORS

4.3.1. All agreements with contractors that permit access to the state information technology infrastructure or access to RPII, CI or SI shall require full collaboration and cooperation with the budget unit for the prompt discovery, mitigation, and closure of incidents involving a suspected data breach consistent with the SISPO Incident Submission and Response Standard, P900-S905, and this standard.

4.3.2. Contractors must provide sufficient information to a budget unit to identify the number of individuals affected by a data breach and how to contract those individuals. Responsibility and collaboration expected from contractors is addressed in the SISPO Incident Submission and Response Standard, P900-S905, section 5.

4.4. RISK ASSESSMENT

4.4.1. When there is suspicion of unauthorized access to a device, record or communication containing restricted personal identifying information (RPII), a budget unit will conduct a risk assessment to determine the potential risk for harm to individuals who may be affected by the incident. The potential risk for harm will determine whether an information security incident is a "data breach" and whether affected individuals must be notified (see section 4.5). At minimum, the following risk factors will be considered in the risk assessment:

4.4.2. Type of RPII. The type of RPII involved in the incident influences the severity of the incident and the potential for risk of harm.

(i) RPII in electronic format has a high risk for use in ID Theft. The state of Arizona recognizes this risk in the Arizona data breach notification law (ARS 44-7501). Other state and federal laws and technology industry standards apply confidentiality protections for data elements defined in the SISPO Information Security Incident Management Policy, P900, and standards as "RPII."[1]

(ii) RPII that is also protected health information (PHI) is required by HIPAA to be safeguarded from unauthorized access. HIPAA applies to RPII contained in any format or medium, including unauthorized access RPII in an oral communication

(iii) When HIPAA does not apply to a budget unit, RPII contained in a non-electronic format or medium is not protected by the Arizona data breach notification law. However, other state or federal laws address safeguard of this information. A risk assessment should be conducted regardless of the format or media that holds the RPII

4.4.3. The Number of Individuals Affected. The number of individuals affected may have a bearing on the risk of harm or the method used for notification. For a breach involving state law, see section 4.6.3. If the breach involves HIPAA data, see HIPAA Appendix A, section 3.

- For example, an inadvertent unauthorized disclosure to a limited number of people that results in the return or proper destruction of the information may not create a significant risk of harm to the individuals whose information was affected by the incident (see 4.4.1(d), exceptions to a data breach). Conversely, one unauthorized disclosure of RPII of any kind may reasonably have the potential to cause significant harm to an individual if the information could result in identity theft.

- The number of individuals affected should not be the determining factor for determining the risk severity of harm from the incident.

[1] The Federal Trade Commission Health Breach Notification Rule for Personal Health Records (16 CFR Part 318), Gramm Leach Bliley Act (Disclosure of Nonpublic Personal Information, Public Law 106-102, Title V Subtitle A , 15 USC, Subchapter I, Sec. 6801-6809; Federal Trade Commission Standards, 16 CFR Part 314), Payment Card Industry (PCI) Data Security Standards.

4.4.4. Likelihood the Information is Accessible and Usable. The reasonable likelihood the incident will allow a non-authorized person to read, decipher, identify, re-identify, use or otherwise gain access to the information is a critical factor for determining a data breach. If the following considerations do not apply, there is a reasonable likelihood the information is accessible and usable. Considerations include:

(i) A device or technology infrastructure component (e.g. a server or printer with digital storage) containing the RPII is recovered and forensic investigation confirms no evidence of unauthorized access of the information in any manner.

(ii) A device or technology infrastructure component is encrypted using a method that meets Arizona Statewide Encryption Technologies Standard, P800-S850. Note: For budget units that comply with HIPAA, see also Department of Health and Human Service's (DHHS) guidance for encryption methodologies published in Federal Register at 74 FR 19006, April 27, 2009 and the Interim Final Rule published in Federal Register at 74 FR 42741, August 24, 2009). The Statewide encryption standard is consistent with the DHHS guidance.

(iii) The information (electronic or non-electronic) is redacted as defined by the Arizona Notification of Breach of Security System (the state breach notification law), ARS 44-7501.[2]

(iv) Electronic media is destroyed or sanitized and renders information contained on the media unusable, unreadable or indecipherable by a non-authorized party (see GITA Media Sanitizing/Disposal Standard, P800-S880, Rev 2.0).[3]

(v) Hardcopy records are destroyed consistent with the Arizona law for Discarding and Disposal of Records, ARS 44-7601.[4]

---

[2] The HIPAA Privacy Rule does not recognize redaction of electronic or non-electronic records as a security method that renders protected health information (PHI) unusable, unreadable or indecipherable (see Federal Register at 74 FR 42742). PHI must be de-identified as defined by the HIPAA De-identification of Protected Health Information Standard 45 CFR 164. 514 or be destroyed (see section 4.4.1, (c)(v) and (vi)).

[3] For agencies that must comply with HIPAA, see also Department of Health and Human Service's (DHHS) guidance for destruction methodologies, published in Federal Register at 74 FR 19006, April 27, 2009 and the Interim Final Rule published in Federal Register at 74 FR 42741, August 24, 2009. The Statewide media destruction standards are consistent with the DHHS guidance.

[4] For agencies that comply with HIPAA, see also Department of Health and Human Service's (DHHS) guidance for destruction methodologies, published in Federal Register at 74 FR 19006, April 27, 2009 and the Interim Final Rule published in Federal Register at 74 FR 42741, August 24, 2009).

(vi) Other methods that meet industry best practices or standards prevent access to the information or to the format, media or device that contains the information (Note, password protection without additional device/component or data security safeguards is not sufficient protection from unauthorized access).

4.4.5. Exceptions to a Data Breach. An information security incident is not a data breach when the investigation reveals the following:

(i) The device, technology infrastructure component or the information contained on a device or component is encrypted, redacted, destroyed or sanitized (see section 4.4.1, (c)(ii),(iii),(iv) and (v))

(ii) There is an unintentional acquisition, access or use of the RPII and the incident investigation finds all of the following:

- The information is accessed by an individual (e.g. workforce member of an budget unit or contractor) performing work within his/her scope of authority or professional relationship;
- The acquisition, access or use is in good faith and not for a personal purpose or gain;
- The event is not a repeat violation of the unauthorized access; **and**
- The individual does not retain or make further use of the information.

(iii) There is an inadvertent disclosure of the RPII and the incident investigation finds all of the following:

- The individual making the disclosure is authorized to access the information and is performing work within his/her scope of authority or professional relationship;
- The disclosure is made to an individual working within the same budget unit or business organization (e.g. employee of a contractor) who is authorized to access the type of information disclosed;
- The act is made in good faith and not for a personal purpose or gain; and
- The recipient does not retain or make further use of the information.

(iv) There is a disclosure of RPII to an unauthorized individual and the budget unit or contractor has a good faith belief that

the unauthorized individual who received the RPII is not reasonably able to retain the information.

4.4.6. Ability to Mitigate the Risk of Harm. Rapid response to an incident may prevent or mitigate further compromise of the information. The mitigation of risk also includes investigative measures taken by a budget unit to determine whether unauthorized access occurred. These measures include one or more of the following:

(i) Recovery of a device, component, or records from a third party accompanied by a signed and dated attestation that confirms the recovery, describes why unauthorized access, including retention of the RPII, did not or could not have occurred

(ii) Forensic analysis of a recovered device or component that confirms unauthorized access to the RPII did not occur (see 4.4.1 (c)(i), Likelihood Information is Accessible and Usable)

(iii) The ability to destroy (wipe) information contained on a device or component after theft or loss (e.g. "kill switch" capability with remote activation)

(iv) Multiple levels of security safeguards or methods to prevent unauthorized access, use or disclosure of information

(v) The timeliness of mitigation measures taken in relation to the timing of the loss or other potential for unauthorized access (e.g. when did the budget unit or contractor lose control of the device, component or record)

(vi) Other factors reasonably likely to prevent or mitigate the risk of unauthorized access or the severity of harm. (Note: password protection without additional device/component or data security safeguards is not sufficient protection from unauthorized access)

4.4.7. Likelihood the Breach May Lead Significant Harm. Using findings from risk assessment factors (a) through (e), the budget unit will determine if the factors taken together pose a risk of substantial financial, reputational or other harm to individuals whose information security or privacy has been compromised by the incident. It is in the best interest of the state to give careful consideration to the threat of harm likely to result from any unauthorized access to RPII regardless of format.

4.4.8. The risk assessment will be conducted as soon as possible but within **30 days** after discovery of the information security incident. The factors considered and findings made during the risk assessment shall become a written record in the budget unit's documentation of the incident. A summary of the risk assessment findings will be added to the incident report in the SISPO IRR system as soon as completed but within **30 days** after discovery of the incident. For additional information see the SISPO Incident Submission and Response Standard, P900-S905, section 4.10).

4.5. DATA BREACH NOTIFICATION

4.5.1. An information security incident will be classified a "data breach" when the budget unit determines through a risk assessment that unauthorized access to RPII poses a substantial risk of harm to individuals whose information is affected by the incident.

4.5.2. A finding of a "data breach" requires a budget unit to determine if data breach notification to affected individuals is mandatory by law or an option that should be considered in the best interest of the state.

4.5.3. Mandatory Notification by Law--Arizona. If the RPII is contained in electronic format and the risk analysis determines the incident poses a substantial risk of harm to affected individuals, the Arizona data breach notification law (ARS 44-7501) will require notification of individuals. The budget unit will use the methods described in section 4.6 for notification of individuals.

4.5.4. Mandatory Notification by Law—HIPAA. If the budget unit complies with HIPAA and the risk assessment determines the incident involves RPII contained in any media or format, including unauthorized access from an oral communication, and poses a substantial risk of harm to affected individuals, HIPAA will require notification of individuals (45 CFR Part 164, Subpart D). The budget unit will use the methods described in Appendix A, section 3.1, to notify individuals.

4.5.5. Optional Notification – Best Interest of the State -- RPII. If the RPII is contained in a non-electronic format or media (i.e. hardcopy record) and HIPAA is not applicable to the budget unit, a risk assessment should be conducted to determine if the incident poses a substantial risk of harm to affected individuals. It is not mandatory under the Arizona data breach notification law to notify individuals for a data breach involving non-electronic records. However, it may be in the best interest of the state and its citizens to notify affected individuals following section 4.6.

4.5.6. Optional Notification – Best Interest of the State – CI or SI. At the option of the budget unit, a risk assessment may be used to determine the level of harm from unauthorized access or communication of Confidential Information or Sensitive Information. If the risk assessment findings indicate the unauthorized

access poses a substantial risk of harm to individuals, it may be in the best interest of the state to notify individuals about the incident. The Arizona data breach notification law does not require notification for unauthorized access of CI or SI. A budget unit may use the methods described in section 4.6.3 and the provisions of section 4.6 for notification of individuals.

4.6. METHODS OF NOTIFICATION

4.6.1. The budget unit shall notify affected individuals when indicated by the outcome of the risk assessment. The notification process will include the collaboration of the budget unit CEO or designee, the budget unit's ISO, APO and, as applicable, HCO; other individuals who will participate in the notification process (e.g. employees and third parties); legal counsel; and SISPO. Law enforcement may also be consulted if a criminal investigation related to the incident could result in a delay of notification (see section 4.6.5).

4.6.2. **HIPAA.** Budget units and their contractors that must comply with HIPAA will follow **Appendix A, section 3, methods of notification required by HIPAA in lieu of section 4.6.3 of the Standard. The budget unit will follow all other sections of 4.6 in the Data Breach Notification Standard**

4.6.3. **Arizona Law**. The Arizona breach notification statute (ARS 44-7501) permits the use of "standard," "substitute" or "alternative" methods to notify individuals. A budget unit will use the most expedient method or methods of notice that are possible.

4.6.4. Standard Notification is used to notify when the budget unit has contact information for the individual. One **or more** of the following methods will be used:

- Non-electronic written notification (e.g. letter or facsimile);
- Electronic notice if this is the primary means used by the Budget Unit to communicate with the individual;
- Telephonic notification;
- A combination of the above.

4.6.5. Substitute Notification is permitted as an option to "Standard Notification" when the cost of standard notification exceeds **$50,000 or** involves more than **100,000** individuals. This method is also permitted when a budget unit lacks sufficient contact information for the affected individuals or class of individuals. Substitute notification requires a budget unit to do all of the following:

(i) Use electronic email notification when the budget unit has email addresses for the individuals;
(ii) Conspicuously post the notification on the budget unit's website;

(iii) Publish the notification to a major statewide media (e.g. news station, news paper, etc).

4.6.6. Alternative Method of Notification**.** A budget unit may use another method of notification consistent with this standard when both of the following are met:

(i) The method is documented in the budget unit's information security and privacy policy, implemented as n budget unit-wide practice and incorporated into written business partner and contractor responsibilities.

(ii) The budget unit is required to comply with federal law, regulation or industry standard for data breach procedures, the method is documented in the budget unit's information security and privacy policy, procedures and practices implemented as an budget unit-wide practice and incorporated into written business partner and contractor (e.g. Payment Card Industry Data Security Standards; Gramm, Leach, Bliley Act and regulatory guidance also known as the Financial Modernization Act of 1999; or the Federal Trade Commission Health Breach Notification Rule (i.e. Personal Health Records Standard).[5]

4.6.7. **Timing of Notification**. Notification to affected individuals or class of individuals shall occur without unreasonable delay and **no later than 60 days after discovery** of the information security incident that caused the data breach.

4.6.8. **Delay of Notification for Criminal Investigation**. A budget unit may delay notification to affected individuals or publication to the media when it receives a written request from a law enforcement agency with jurisdiction in Arizona or from the Arizona Attorney General's Office (AGO) that public notification will impede a criminal investigation related to the information security incident. The budget unit will notify SISPO of the delay and consult with its legal counsel regarding the request. Additionally, every **30 days or more frequently as updates occur,** the budget unit shall:

(a) Evaluate and document the necessity of the additional delay with the requesting law enforcement agency or the AGO.

(b) Determine if the delay of notification is reasonably likely to significantly escalate the risk of harm to the affected individual(s).

(c) Promptly notify the law enforcement agency or the AGO, or both, and determine the earliest possible date when notification of individuals may occur to remediate the risk of harm.

[5] HIPAA Standard: *Breach Notification for Unsecured Protected Health Information,* 45 CFR Part 164, Subpart D.

(d) Notify SISPO of escalation of the risk of harm and collaborate with SISPO and the budget unit's incident response team to remediate the risk (see Information Security Incident Management Policy, P900, section 4.3.5).

4.6.9. **Content of Breach Notification Letter**. The notification letter to an individual shall at a minimum address the following:

(a) A brief, factual description of what happened; including when the data breach occurred or was discovered to have occurred;

(b) To the extent possible, a description of the elements of information involved in the breach (e.g. first and/or last name, social security number, driver license number, non-operator identification number, account/financial/credit/debit number, account access password/PIN/code, etc);

(c) A statement of how/whether the information was encrypted or protected to the extent such information does not compromise information management security (e.g. data encrypted or redaction of hardcopy records);

(d) Additional information that provides benefit to the individual to assess his/her risk of harm from the incident (e.g. if information was retrieved or the likelihood of an unauthorized party accessing, using or retaining the information);

(e) What steps the individual should take to protect him/her from potential harm (e.g. credit report review, credit monitoring, etc);

(f) A description of what the budget unit is doing individually, in collaboration with its business partner(s) or contractor(s), with other budget units (if a multi-budget unit response) or SISPO to investigate the breach, mitigate losses, and protect against future similar incidents;

(g) How an individual may obtain additional information about the data such as a toll-free telephone number, e-mail address, postal address, home page or link to a support center, and, if applicable, name or title of an office providing support to affected individuals;

4.6.10. Sample letter templates for data breaches that involve financial or medical information are provided in Appendix 2A and 2B of this standard. Information for consumers on protections available from the Arizona Security Freeze law (ARS 44-1698), Appendix 2C, should be added as an attachment to the breach notification sent to individuals.

4.7. COMMUNICATIONS

4.7.1. **Content of Communications.** The budget unit CEO shall ensure that internal and external communications regarding the data breach are consistent with the factual description of the incident and with the content of the notification letter to individuals (see section 4.6.9). A copy of all statements, notification letters and description of the incident shall be retained consistent with the Information Security Incident Management Policy, P900, section 6, Retention of Records.

4.7.2. **Communications Team.** It is recommended that the budget unit CEO appoint a communications team to manage internal and external communications about the incident. The incident management team may be able to assume this role. The team should be under the direction of the budget unit public information officer (PIO) (see SISPO Information Security Incident Management Policy, P900, section 4.3.5).

4.7.3. **Internal Communications.** When there will be a public notification (e.g. to individuals or the media) about a data breach, it is recommended that the budget unit CEO authorize the public information officer to issue a communication to the budget unit workforce. The communication should be made available to the workforce prior to the matter becoming public. It is recommended that the internal communication address:

(a) The basic facts of the incident (e.g. what happened, what data was exposed and to whom, if relevant) consistent with section 4.6.9 (content of notification letter) and the SISPO incident report;

(b) Steps the budget unit is taking to mitigate harm;

(c) Where the workforce can direct questions or obtain information;

(d) Special recognition by workforce or contractors who response to the incident averted harm or re-occurrence;

(e) Steps the budget unit is taking to prevent a re-occurrence and whether these actions will be visible to workforce (e.g. new policies/procedures, training, equipment or software upgrades (e.g. laptop encryption).

4.7.4. **Communications with Affected Individuals**. The budget unit shall collaborate with the communications team in (see section 4.7.2) to develop a response management plan to handle inquiries about the incident from affected individuals. The response management plan will consider the number of individuals affected, the types of questions the individuals may ask, resources where the individuals may obtain assistance to assess and manage their personal risk (e.g. contact information for credit monitoring services, options for a security freeze, and other guidance approved by the team). Communications with affected individuals should follow a written script or other communication guide

consistent with the content of the notification letter, the Arizona Security Freeze law (See Exhibit 2C).

4.7.5. **Additional Considerations for Communications**. The budget unit may also consider the following for communicating with affected individuals:

(a) It is recommended that the budget unit develop a written script or other communication guide for workforce or other individuals at the state who, in addition to the budget unit's PIO, are authorized by the budget unit or the state to respond to inquiries from the media about the incident.

(b) A budget unit may benefit by using a centralized call center, prepared scripts, call logs and trained personnel for response to a data breach that involves a significant number of affected individuals. Governance of call center activities will be coordinated with the budget unit PIO.

4.7.6. The budget unit will coordinate its communication plan with SISPO, the Government Information Technology Director of Communication and state executive leadership.

4.8. CORRECTIVE ACTION AND ENFORCEMENT

The need for corrective action and enforcement will be a factors considered for mitigation of the incident (see Information Security Incident Management Policy, P900, section 5).

4.9. RETENTION OF RECORDS

See Information Security Incident Management Policy, P900, section 6.

4.10. AUTHORITIES

- ARS 41-3507 – Duties, Statewide Information Security and Privacy Office
- EO 2008-10 – Executive Order, Mitigating Cyber Threats
- ARS 41-3504 – Powers and Duties of the Agency
- ARS 13-2301(E)(2) – Computer Tampering
- ARS 44-7501 – Notification of Breach of Security System (AZ Data Breach Law)
- ARS 44-7601 – Discarding and Disposal of Records
- 45 CFR Parts 160, 162 and 164 – Rules for the Health Insurance Portability and Accountability Act of 1996 and as amendment by the Health Information Technology for Clinical and Economic Health Act, 2009
- Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007

APPENDIX A
SISPO INFORMATION SECURITY INCIDENT DATA BREACH STANDARD

HIPAA[6] DATA BREACH NOTIFICATION

1. BACKGROUND

In February 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed by Congress as part of the American Recovery and Reinvestment Act (ARRA). The HITECH law required the Department of Health and Human Services (DHHS) and it's Office for Civil Rights (OCR), the enforcement agency for HIPAA, to issue updated regulations consistent with HITECH.

HITECH enacted a significant change to the HIPAA privacy and security rule in its requirement that covered entities and business associates promptly identify and respond to a data breach of "unsecured"[7] protected health information or "PHI" (also defined by the SISPO Information Security Incident Management Policy, P900, and Standards as "RPII").

The HITECH Act requires a covered entity to report data breaches of unsecured PHI to the individual (to whom the PHI belongs), to the U.S. Department of Health and Human Services and to the media if the breach involves 500 or more individuals.

2. SCOPE

Appendix A applies to a budget unit or a component of a budget unit defined as a HIPAA covered entity or component that must notify an individual or individuals of a data breach involving unsecured PHI. Contractors, who are "business associates" of a budget unit, as defined by HIPAA, will collaborate with the budget unit to identify, mitigate and respond to a data breach of PHI and provide contact information or other assistance as may be needed by a budget unit to notify an individual, DHHS or the media of the breach.

3. STANDARD

The budget unit and its business associate(s) will comply with the SISPO Data Breach Notification Standard to identify, mitigate and respond to a data breach of PHI. In addition to this Data Breach Standard, a budget unit will use the methods described in Appendix A to notify an individual and DHHS of a data breach involving PHI. A business associate will also follow Appendix A for purposes of notification of affected individuals if by agreement with the budget unit the business associate will provide the

---

[6] References to HIPAA mean the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as amended b the American Recovery and Reinvestment Act of 2009 (Pub.L No. 111-5) (the "HITECH Act") any associated regulations and the federal regulations published at 45 CFR Parts 160 and 164 (collectively referred to as "HIPAA").

[7] The DHHS Guidance published in the Federal Register on April 27, 2009 lists and describes encryption and destruction as the two technologies and methodologies for security PHI and the information unusable, unreadable, or indecipherable to unauthorized individuals. This guidance is currently found at the following website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.

data breach notification. The budget unit will collaborate with SISPO for the management and resolution of the breach until incident closure.

3.1 **Notification of Individuals**

A budget unit that complies with HIPAA will use the methods listed in 3.2.1 or 3.1.1 to notify an individual or individuals of a data breach The budget unit will collaborate with SISPO for the data breach notification and management of notification of individuals and, if applicable, to the media .

3.1.2 Notification by Written Methods. A budget unit may use the following methods to provide notice of a data breach an individual or a decussated individual's next of kin or personal representative. Notification may be provided in one or more mailings as information becomes available:

(a) To an Affected Individual. A letter sent by first class mail to the individual's last known address. Alternatively, the budget unit may use electronic notice if the individual agrees to this method and has not withdrawn agreement to this form of notice

(b) For Deceased Individual. Notice by first class mail to the personal representative or next of kin when the budget unit has the last known address for the next of kin or personal representative. However, a budget unit does not need to notify a next of kin or personal representative when the contact information is insufficient or out-of-date and precludes written notification to the next of kin or personal representative.

3.1.3 Substitute Methods of Notification. When there is insufficient or out-of-date contact information for an individual affected by a data breach, the budget unit may use a substitute form of notice reasonably calculated to reach the individual. The following methods of substitute notice are permitted by HIPAA:

(a) For 10 or Fewer Individuals. The budget unit may provide substitute notice using an alternative form of written notice, telephone or other means of notice.

(b) For 10 or More Individuals. The budget unit shall provide substitute notice by doing the following:

(i) Publish a conspicuous notice for **90** days on the home page of the website for the HIPAA covered budget unit or covered component website, whichever will best reach the affected individual(s)

(ii) In the alternative, the budget unit may publish a conspicuous notice in major print or broadcast media in

geographic areas where the affected individual(s) likely reside

(iii) In addition to publishing a conspicuous notice as described in b (i) or b (ii), the budget unit shall provide a toll-free phone number that remains active for at **least 90 days** where an individual can learn whether his/her information may be affected by the data breach.

(c) Additional Notice in Urgent Situations. If a budget unit determines notification is urgent because of possible imminent misuse of the unsecured PHI, information may also be provided to an individual by telephone or other means, as appropriate, in addition to the written notification discussed in 3.2.1(a).

3.2 Notification of DHHS and Media

The Department of Health and Human Services (DHHS) requires a covered entity to notify DHHS of a data breach. The timing of notification depends on the number of individuals affected by the breach. The budget unit will collaborate with SISPO for submission of data breach notification to DHHS.

3.2.1 Data Breach Affects Less than 500 Individuals.

(a) A budget unit shall notify DHHS of each incident that occurred during a calendar year. The notice(s) must be submitted using the DHHS online submission process or as otherwise prescribed by DHHS and submitted **not later than 60 days after the** end of the year in which the breach occurred. A budget unit is not required by DHHS to notify the media for a breach affecting less than 500 individuals.

(b) The budget unit will maintain a log or other documentation (i.e., the SISPO IRR system incident report) for each data breach occurring during the year.

(c) SISPO may coordinate with HIPAA covered budget units for notification to DHHS. SISPO may also, with agreement of the budget unit, submit notification to DHHS acting on behalf of the state and the budget unit.

(d) A copy of the DHHS notification will be made an attachment to the incident report entered by the budget unit in the SISPO Incident Reporting and Response (IRR) system.

3.2.2 Data Breach Affects 500 or More Individuals in the Same State or Jurisdiction.

(a) Media. A budget unit shall notify prominent media outlets serving the state or jurisdiction following the discovery of the data breach. Unless a delay is requested by law enforcement (see Data Breach Notification Standard section 4.6.5), notification shall occur **without unreasonable delay and not later than 60 days after discovery of a breach**. The content of the notification will meet the requirements of the SISPO Data Breach Notification Standard section 4.6.6.

(b) DHHS. A budget unit shall notify DHHS of the data breach **contemporaneously** with the breach notification provided to the affected individuals unless a delay is requested by law enforcement. The notice must be submitted using the DHHS online submission process or as otherwise prescribed by DHHS.

(c) SISPO may coordinate with HIPAA covered budget units for notification to DHHS. SISPO may also, with agreement of the budget unit, submit notification to DHHS acting on behalf of the state and the budget unit.

(d) A copy of the DHHS notification will be made an attachment to the incident report for the data breach entered by the budget unit in the SISPO Incident Reporting and Response (IRR) system.

3.3 Data Breach of Personal Health Records

Budget units and business associates that maintain personal health records (PHR) or support PHR systems must also comply with the safeguard and breach notification requirements issued by the Federal Trade Commission (See 16 CRF Part 318; 74 FR 42962 to 42986 at http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf).

Appendix2A
SISPO Data Breach Standard

Sample Breach Notification Letter -- Financial

Instructions: This letter template may be used by a state budget unit to notify individuals about a data breach. Another format consistent with the Data Breach Notification Standard, section 4.6.9 may be used by the budget unit.

Content Format Key:

Bold Font – Recommend language be included in the letter.
Underlined Italics – Add content specific to the incident.
Optional – Additional content to clarify risk exposure to the individual or the additional steps the budget unit is taking to answer questions or reduce risk of harm to individuals (e.g. credit monitoring or ID Theft protection services). Please note that the Arizona and HIPAA breach notification requirements do not require an organization/budget unit to pay for credit monitoring or ID Theft protection services.

[Budget unit Letterhead]

[Date of Notification Letter]

An Important Message for Our Customers:

[**Optional**-specific salutation: "Dear _____" or other salutation]

On [*insert date incident occurred or was discovered***] our agency** *[and/or contractor/business associate/business partner***] experienced** *[briefly describe the information security incident in plain terms such as a "loss, theft, or access by a person not authorized to receive the information"***]. The agency's investigation indicates that information involved in the** *[incident, theft, loss, etc]* **is believed to include your [***list as specifically as possible what type of RPII, CI or SI was breached]*. **The** *[information or type of device or media*] **involved** [*was/was not*] **encrypted** *[or other protection used such as redaction or destruction of data*].

We are fully investigating this incident [*Describe briefly what the budget unit and or /its contractor is doing to investigate the breach, steps taken to mitigate the harm to individuals, and to protect against further unauthorized access or loss. Include information such as recovery of device or records, forensic testing for unauthorized access/duplication, or other reason information may not have been accessible or retained by an unauthorized third party*].

Because of the type of information involved with this incident, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. We suggest you call or write to one of the four credit

reporting agencies below to request that a fraud alert be placed on your credit file. A fraud alert lets creditors know to contact you before opening new accounts.

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/home	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	**TransUnion Security Freeze** P.O. Box 6790 Fullerton, CA 92834-6790 1-888-909-8872 www.transunion.com	**INNOVIS** 1-800-540-2505 https://www.innovis.com/.h

A fraud alert can be placed with any of these agencies at no cost to you. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each. A fraud alert lasts for 90 days.

When you receive your credit reports look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Also look for personal information, such as your home address, spelling of your name, social security number or other identifier which is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Even if you do not find any signs of fraud on your reports, you may want to check your credit report periodically for several months. Just call one of the numbers above to order your reports and keep the fraud alert in place.

If you have placed a fraud alert, but still believe you are at risk, Arizona law (ARS 44-1698) allows a consumer to place a security freeze (also called a "credit freeze") on your credit file. A security freeze means that you must authorize a credit reporting agency to share your credit file and/or credit score with potential creditors before new credit cards or other lines of credit can be opened. For more information on Arizona Security Freeze law, please refer to the attached information sheet.

If you have any questions about the information provided in this letter, please contact [*insert phone number*] .

[**Optional:** Describe other steps the budget unit is taking to assist individuals, such as web link for further information or questions. An budget unit may choose to offer a paid credit monitoring services (e.g. monitor credit activity and scores) or identify theft protection services (e.g. monitor credit activity/scores and provide ID theft resolution services) to individuals who verify the breach resulted in ID theft or other financial harm. Alternatively, the budget unit may find the risk of harm significant and offer a paid service to all individuals notified of the breach unless the individual declines in writing.]

Sincerely,

[*Name and Title of Budget unit Representative*]

[**Optional**: "cc" as determined by budget unit]

bcc: Agency -- one copy of letter template for budget unit incident file; attach with list of individuals notified
SISPO -- one copy of letter template for SISPO IRR system incident record
Other distribution as determined by budget unit

Appendix 2B
SISPO Data Breach Standard

Sample Breach Notification Letter -- Medical

Instructions: This letter template may be used by a state budget unit to notify individuals about a data breach. Another format consistent with the Data Breach Notification Standard, section 4.6.9 may be used by the budget unit.

Content Format Key:
Bold Font – Recommend language be included in the letter.
Underlined Italics – Add content specific to the incident.
Optional – Additional content to clarify risk exposure to the individual or the additional steps the budget unit is taking to answer questions or reduce risk of harm to individuals (e.g. credit monitoring or ID Theft protection services). Please note that the Arizona and HIPAA breach notification requirements do not require an organization/budget unit to pay for credit monitoring or ID Theft protection services.

[Budget unit Letterhead]

[Date of Notification Letter]

An Important Message for Our Customers:

[**Optional**--specific salutation: "Dear _____" or other salutation]

On [*insert date incident occurred or was discovered***] our agency** *[and/or contractor/business associate/business partner***] experienced** *[briefly describe the information security incident in plain terms such as a "loss, theft, or access by a person not authorized to receive the information"***]. The agency's investigation indicates that information involved in the** *[incident, theft, loss, etc]* **is believed to include your [***list as specifically as possible what type of RPII, CI or SI was breached]*. **The** *[record, type of device or media*] **involved** [*was/was not*] **encrypted** *[or other protection used such as redaction or remote destruction of data*].

We are fully investigating this incident [*Describe briefly what the budget unit and or /its contractor is doing to investigate the breach, steps taken to mitigate the harm to individuals, and to protect against further unauthorized access or loss. Include information such as recovery of device or records, forensic testing for unauthorized access/duplication, or other reason information may not have been accessible or retained by an unauthorized third party*].

[Medical -- *If applicable*--"The type of information lost could be useful to bill for medical services you did not receive. You may wish to check with Member Services at your health insurance plan to make sure that the services billed since [*insert date or time frame of breach*] are ones that you received. Also, please report any services found on health plan

statements or explanation of benefits that you did not receive. This may be evidence of Medical ID Theft. Medical Identity Theft is a crime. It occurs when an ID thief receives medical care that is billed to your health plan as care you received. If you see medical care on statements you question receiving, please do the following:

- **Contact your health plan customer service center. Make sure that only services you received are in your history. You can request correction of your records if you find that there are services that you did not receive according to your records.**
- **Read your insurance statements. Make sure that they only list services that you received. Contact your health plan customer service center about services you did not receive. Ask that your billing record be corrected.**
- **Contact your health care provider if you receive bills for services you did not get. Ask about how to correct your medical record."]**

[Financial -- if applicable-- "Because the information also involved financial related information, you may want to place a fraud alert on your credit file. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A call to one agency will automatically place an alert with all of the other agencies. A fraud alert lets creditors know to contact you before opening new accounts.]

We also suggest you call one of the below listed credit agencies to place a fraud alert on your credit file:

Equifax **Security Freeze** P.O. Box 105788 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/home	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	**TransUnion Security Freeze** P.O. Box 6790 Fullerton, CA 92834-6790 1-888-909-8872 www.transunion.com	**INNOVIS** 1-800-540-2505 https://www.innovis.com/.h

A fraud alert can be placed with any of these agencies at no cost to you. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each. A fraud alert lasts for 90 days.

When you receive your credit reports look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Also look for personal information, such as your home address, spelling of your name, social security number or other identifier which is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Even if you do not find any signs of fraud on your reports, you may want to check your credit report periodically for several months. Just call one of the numbers above to order your reports and keep the fraud alert in place.

If you have placed a fraud alert, but still believe you are at risk, Arizona law (ARS 44-1698) allows a consumer to place a security freeze (also called a "credit freeze") on your credit file. A security freeze means that you must authorize a credit reporting agency to share your credit file and/or credit score with potential creditors before new credit cards or other lines of credit can be opened. For more information on Arizona Security Freeze law, please refer to the attached information sheet."]

If you have any questions about the information provided in this letter, please contact [*insert phone number*] .

[**Optional:** Describe other steps the budget unit is taking to assist individuals, such as web link for further information or questions. An budget unit may choose to offer a paid credit monitoring services (e.g. monitor credit activity and scores) or identify theft protection services (e.g. monitor credit activity/scores and provide ID theft resolution services) to individuals who verify the breach resulted in ID theft or other financial harm. Alternatively, the budget unit may find the risk of harm significant and offer a paid service to all individuals notified of the breach unless the individual declines in writing.]

Sincerely,

[*Name and Title of Budget unit Representative*]

[**Optional**: "cc" as determined by budget unit]

bcc: Agency -- one copy of letter template for agency incident file; attach with list of individuals notified
SISPO -- one copy of letter template for SISPO IRR system incident record
Other distribution as determined by budget unit

Appendix 2C
SISPO Data Breach Standard

[Attachment to Breach Notification Letter-Financial or Medical]

ARIZONA SECURITY FREEZE LAW[1]
GENERAL INFORMATION

Arizona has a security freeze law (Arizona Revised Statute § 44-1698). This law allows a consumer to place a security freeze on his or her credit report and credit score by sending a written request to a credit reporting agency.

When a freeze is in place with a credit bureau, any changes in a consumer's name, date of birth, Social Security number or address must also be confirmed with the consumer by the credit bureau 30 days before the change is posted to their file. The four credit bureaus have slightly different requirements, so please carefully review the process for each. The service to place the security freeze is free if you are a victim of an actual identity theft crime. To prove you are a victim, you must send a valid copy of a police report, a law enforcement investigative report or a written complaint to the Federal Trade Commission. If the Security Freeze is not free, a charge of $5 or more will be applied for each time you place, remove or temporarily lift the freeze. Be prepared to provide the following information to the credit reporting agency to request a Security Freeze:

- If you are a victim of identity theft, you must include a copy of either the police report or case number documenting the identity theft
- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth
- If you have moved in the past 5 years, supply the addresses where you have lived over the prior 5 years
- Provide proof of current address such as a current utility bill or phone bill
- Send a photocopy of a government issued identification card (state driver’s license or ID card, military identification, etc.)

Consumers should carefully consider whether a Security Freeze is right for them. Consumers should plan ahead to arrange to remove the freeze before seeking a loan or new credit. A Security Freeze does not apply to numerous entities, including government agencies in matters related to child support or delinquent taxes.

Contact the following Credit Reporting Agencies to request a Security Freeze:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/home	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	**TransUnion Security Freeze** P.O. Box 6790 Fullerton, CA 92834-6790 1-888-909-8872 www.transunion.com	**INNOVIS** 1-800-540-2505 https://www.innovis.com/.h

For additional information about the Arizona Security Freeze Law, please see the Arizona Attorney General's Office website at http://www.azag.gov/consumer/SecurityFreeze/index.html.

You may also contact the following for additional assistance:

Crime, Fraud & Victim Resource Center Arizona Attorney General's Office 1275 West Washington Street Phoenix, Arizona 85007	602.542.2123 (Phoenix) 520.628.6504 (Tucson) 800.352.8431 (toll free in State of Arizona, outside Maricopa and Pima Counties) 602.364.1970 (fax) communityservices@azag.gov

[1] Suggested content for Exhibit 2C obtained from the Attorney General's Office website at: http://www.azag.gov/consumer/SecurityFreeze/index.html.

---

[i] References to HIPAA mean the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as amended b the American Recovery and Reinvestment Act of 2009 (Pub. L No. 111-5) (the "HITECH Act") any associated regulations and the federal regulations published at 45 CFR Parts 160 and 164 (collectively referred to as "HIPAA").