



**ADOA - ASET**

Arizona Strategic Enterprise Technology

## Arizona Health Information Exchange (HIE)

### PIN 003 – Privacy & Security

**CFDA #:** 93.719

**Opportunity #:** EP-HIT-09-001

---

**Updated:** 06/01/2012

**Prepared By:**

The Arizona Strategic Enterprise Technology Office

## **PIN 003 – Privacy & Security**

### **Table of Contents**

Template 1 .....	3
Template 2 .....	5
Attachments .....	10

## PIN 003 – Privacy & Security

### Template 1

#### HIE Architectural Model: Point-to-Point Directed Exchange

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
<b>Required to address</b>			
	Referenced policies are found in the attached document: ARIZONA Response – PIN 003 – Privacy & Security - Attachments  Doc Ref. #1: Arizona Health Information Exchange Marketplace Requirements and Specifications Health Information Service Provider (HISP)		
<b>Openness and Transparency</b>	HISP Vendors will certify to AzHeC and the customer that it has established a breach notification compliance program which requires timely notice to customer as required by law and that it will adhere to all requirements that will prevent a breach. (Doc #1 PS #3 pg.7)	Contract with AzHeC to provide communication and education. This is part of the overall Arizona HIE Marketplace contract with AzHeC.  Policies for HISP vendors are available at: <a href="http://www.azhec.org/resource/resmgr/files/arizona_hie_marketplace_requ.pdf">http://www.azhec.org/resource/resmgr/files/arizona_hie_marketplace_requ.pdf</a>	None
<b>Collection, Use and Disclosure Limitation</b>	HISP Vendors will comply with all applicable Arizona and federal privacy and security laws and regulations. (Doc #1 PS #1 pg. 6)  HISP vendors will be compliant with HIPAA and HITECH Privacy and Security rules. (Doc #1 PS #4 pg. 7)	Included in policies for HISP vendors – see link above	None

## PIN 003 – Privacy & Security

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
<b>Safeguards</b>	HISP vendors will complete a security audit and penetration test on their technology infrastructure and provide documented results to Arizona customers. The security audit and penetration test must be repeated on a regular basis as required by law and no less frequently than annually and as there are significant technology infrastructure changes. HISPS will also notify their customers of major findings and corrective actions and all known breaches. (Doc #1 PS #5 pg. 7)	Included in policies for HISP vendors – see link above	None
<b>Accountability</b>	HISP vendors will execute a contract/business agreement with customer which includes privacy and security obligations and indemnifies the customer against a breach that the HISP is solely responsible for. (Doc #1 PS# 2 pg. 7)	Included in policies for HISP vendors – see link above	None
<b>Optional to address</b>			
<b>Individual Access</b>	N/A		
<b>Correction</b>	N/A		
<b>Individual Choice</b>	N/A		
<b>Data Quality and Integrity</b>	N/A		

## PIN 003 – Privacy & Security

### Template 2

**HIE Architectural Model: Data Aggregation (HIE entities that store, assemble, or aggregate individually identifiable health information, whether centrally or in a federated model)**

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
<b>Required to address</b>			
	<p style="text-align: center;"><b>Privacy and Security Policies Health Information Network of Arizona (HINAz)</b></p> <p>Referenced policies are found in the attached document: ARIZONA Response – PIN 003 – Privacy &amp; Security - Attachments</p> <p><u>Doc Ref. #2:</u> Privacy, Security and Individual Rights in the Health Information Network of Arizona</p> <p><u>Doc Ref. #3:</u> Patient Consent to Participate in the Health Information Network of Arizona</p>	<p style="text-align: center;"><b>State Statute</b></p> <p>Referenced statutes are found in attached documents:</p> <p><u>Doc Ref. #4:</u> HB 2620 – Enacted in 2011</p> <p><u>Doc Ref. #5:</u> HB 2369 – Enacted in 2012</p>	

## PIN 003 – Privacy & Security

Domain	Description of approach and where domain is addressed in policies and practices		Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
<b>All Domains</b>			<p>Communication plans are included in the overall HINaz marketing and communications campaign.</p> <p>General Privacy and Security information available on HINaz website at <a href="http://www.HINaz.org">www.HINaz.org</a></p>	
<b>Individual Access</b>	Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)  <u>Section A</u> (Doc Ref. #2) - 4.1 Individual Access (pg. 7)	HB 2369 (Doc Ref. #5)  <u>12-2293</u> Release of medical records and payment records to patients and health care decision makers; definition	See Above	None
<b>Correction</b>	Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)  <u>Section A</u> (Doc Ref. #2) - 2.5 Amendment of Data (pg. 6) - 4.2 Amendment of Data (pg. 8)	HB 2369 (Doc Ref. #5)  <u>36-3802</u> Individual rights	See Above	None
<b>Openness and Transparency</b>	Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)	HB 2369 (Doc Ref. #5)  <u>36-380</u> Notice of health information	See Above	None

## PIN 003 – Privacy & Security

Domain	Description of approach and where domain is addressed in policies and practices		Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
	<p><u>Section A</u> (Doc Ref. #2)</p> <ul style="list-style-type: none"> <li>- 1.5 Notice of Privacy Practices (pg.6 )</li> <li>- 4.3 List of Persons who have Accessed Data (pg. 8)</li> <li>- 4.4 Breach Reporting (pg. 8)</li> </ul>	<p>practices</p> <p><u>36-3802</u> Individual rights</p>		
<b>Individual Choice</b>	<p>Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)</p> <p><u>Section A</u> (Doc Ref. #2)</p> <ul style="list-style-type: none"> <li>- 1.8 Individuals Who Opt Out (pg.5 )</li> <li>- 1.13 Individual Rights (pg. 6)</li> <li>- 2.2 Individual Consent to Disclose to Network (pg. 7)</li> </ul> <p>Patient Consent to Participate in the Health Information Network of Arizona (Doc Ref. #3 Pgs. 1-3)</p>	<p>HB 2369 (Doc Ref. #5)</p> <p><u>36-380</u> Notice of health information practices</p> <p><u>36-380</u> Voluntary participation in health information organizations</p> <p>HB 2620 (Doc Ref. #4)</p>	See Above	None
<b>Collection, Use and Disclosure Limitation</b>	<p>Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)</p> <p><u>Section A</u> (Doc Ref. #2)</p> <ul style="list-style-type: none"> <li>- 1.1 Use of Data for Operation and Maintenance of Network (pg. 3)</li> <li>- 1.2 Use of Data for Permitted Use (see Definition #12 for “Permitted Use”) (pg. 3)</li> <li>- 1.3 Use of Data with Permission of Data Supplier (pg. 3)</li> <li>- 1.4 Response to Subpoenas, Court Orders or Governmental Requests (pg. 3)</li> </ul>	<p>HB 2369 (Doc Ref. #5)</p> <p><u>12-2294</u> Release of medical records and payment records to third parties</p> <p><u>36-3805</u> Disclosure of individually identifiable health information</p>	See Above	<p>HINAz has not yet identified its Privacy Officer.</p> <p>HINAz will designate a Privacy Officer by Fall 2012.</p>

## PIN 003 – Privacy & Security

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
	<ul style="list-style-type: none"> <li>- 1.6 Sale or Commercial Use (pg.6 )</li> <li>- 1.7 Transfers of Data for Research (pg.6 )</li> <li>- 1.8 Use or Disclosure of Individually Identifiable Health Information(pg. 8)</li> <li>- 1.11 Minimum Necessary Standard (pg.9 )</li> <li>- 2.3 Information Subject to Special Protection (pg. 5)</li> <li>- 3.4 Access Only for Permitted Use (pg. 7)</li> <li>- 3.5 Amount of Data Accessed (pg. 7)</li> </ul>		
<b>Data Quality and Integrity</b>	Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)  <u>Section A</u> (Doc Ref. #2) - 2.4 Quality of Information (pg. 5)	HB 2369 (Doc Ref. #5)  <u>36-3806</u> Required policies	See Above  None
<b>Safeguards</b>	Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)  <u>Section A</u> (Doc Ref. #2) - 3.2 Identification and Authentication of Authorized Users (pg. 6)  <u>Section B</u> (Doc Ref. #2) - 1.1 - 1.2 Designated Security Personnel (pg. 13) - 2.1 - 2.3 HINAz Email (pgs. 13-14) - 3.1 - 3.2 HINAz Faxes (pg. 14) - 4.1 - 4.2 Required Vendor Security Policy (pgs. 14-15)	HB 2369 (Doc Ref. #5)  <u>36-3806</u> Required policies	See Above  HINAz has not yet identified its Security Officer.  HINAz will designate a Security Officer by Fall 2012.



## PIN 003 – Privacy & Security

Domain	Description of approach and where domain is addressed in policies and practices		Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing
<b>Accountability</b>	Privacy, Security and Individual Rights in the Health Information Network of Arizona (Doc Ref. #2)  <u>Section A</u> (Doc Ref. #2) - 5.1 Participant Reporting (of Breach) (pgs. 9-10) - 5.2 HINaz Reporting (of Breach) (pgs.10-13) - 5.3 Mitigating Effects of Non-Compliance (pg. 13) - 5.4 Enforcement (pg. 13)  <u>Section C</u> (Doc Ref. #2) - 1.1 - 1.6 Investigation of Individual Complaints, Breaches of Unsecured PHI (pgs. 15-16 ) - 2.1 - 2.3 Participant Required Actions (pgs. 16-17) - 3.1 - 3.2 Auditing and Compliance (pg. 17)	HB 2369 (Doc Ref. #5)  <u>36-3805</u> Disclosure of individually identifiable health information	See Above	None

## **PIN 003 – Privacy & Security**

### **Attachments**

Attachments are found in a separate document:

ARIZONA Response – PIN 003 – Submitted 06-01-2012 – Attachments

#### **Attachments Table of Contents**

Doc Ref. #1: Arizona Health Information Exchange Marketplace Requirements and Specifications Health Information Service Provider (HISP)

Doc Ref. #2: Privacy, Security, and Individual Rights in the Health Information Network of Arizona

Doc Ref. #3: Patient Consent to Participate in the Health Information Network of Arizona

Doc Ref. #4: HB 2620 – Enacted in 2011

Doc Ref. #5: HB 2369 – Enacted in 2012