



ARIZONA DEPARTMENT OF HEALTH SERVICES

PREPAREDNESS

Greetings!

Welcome to the Ryan White team!

Attached are the start-up forms for Arizona's HIV Care and Services data systems and web portals. Depending on what you need, different forms are required.

Required Forms:

EVERYONE:

- User Confidentiality Agreement
- User Acceptable Use
- Acceptable Use 005 Policy –included for reference, you do not need to sign.

If you want CAREWare for recording client services and financial data entry, please add:

- CAREWare User Agreement

If you would like access to internal policies, billing submissions, site visit documents and general reports, add:

- HSP User Agreement

Next Steps:

Submit HAND-SIGNED forms to CAREWaresupport@azdhs.gov. We are sad to share that ADHS IT does not yet accept electronic signatures.

Within 3 business days of receiving your forms, you can expect customized instructions for accessing the data systems, setting up your password (maybe twice!), and CAREWare installation, as appropriate.

Questions?

Please email CAREWaresupport@azdhs.gov or call 602.364.3615.

Warm regards,

The Arizona Ryan White Part B and ADAP team.

Douglas A. Ducey | Governor Cara M. Christ, MD, MS | Director

ARIZONA DEPARTMENT OF HEALTH SERVICES
Confidentiality Agreement Form

PLEDGE TO PROTECT CONFIDENTIALITY INFORMATION

I, _____, understand and agree to abide by the following statements addressing
(Please Print Name)

the creation, use and disclosure of confidential information, including information designated as protected health information (“PHI”), and all other sensitive information:

1. I understand that as a user of information at the Arizona Department of Health Services, I may develop, use, or maintain information relating to public health and welfare, direct or indirect health care, quality improvement, peer review, audit functions, education, billing, reimbursement, administration, research or other approved purposes. This information, from any source and in any form, including, but not limited to paper records, oral communications, audio recordings and electronic display, is considered confidential. Access to confidential information is permitted only on a need-to-know basis and limited to the minimum amount of confidential information necessary to accomplish the intended purpose of the use, disclosure or request.
2. I understand that it is the policy of the Arizona Department of Health Services that users (i.e. employees, medical staff, students, volunteers, contractors, vendors and others who may function in an affiliated capacity) shall respect and preserve the privacy, confidentiality, and security of confidential information.
3. I understand that persons who have access to information that contains confidential information are ethically and legally responsible for observing the federal and state statutes and rules governing confidential records. I will not alter, misuse, disclose without proper authority or the individual’s authorization any confidential information.
4. I understand that confidential information may include oral communications, paper or electronic documents, databases, audio/visual tapes, and other items identified as “confidential” or “sensitive” information.
5. I understand that Arizona State Law prohibits me from using confidential information for personal gain.
6. I understand that confidential information in my control must be maintained and protected from inappropriate disclosure at all times (i.e. hard copy information when not in use will not be accessible to others, including stored or locked or other secure compartments, computer files must be password protected and closed, working documents turned face down on desk, electronic transmission of information will be encrypted according to Department policy, etc.)

ARIZONA DEPARTMENT OF HEALTH SERVICES
Confidentiality Agreement Form

7. I understand that it is the user's responsibility to protect highly sensitive Department information. As such, I am required to use good judgment in assessing what form of communication is appropriate for particular information. If I have any questions or concerns, I am to consult Department policies, my supervisor or the applicable Assistant Director for guidance.
8. I understand that confidential information may only be accessed when I am specifically authorized to do so by the appropriate program manager and I will use only the amount of information necessary within the scope of my duties. When confidential information is no longer needed, I will dispose of it in an appropriate manner to prevent inappropriate access to that information.
9. I understand that confidential information, including paper and electronic records, correspondence, documents and other forms of such information, cannot be released to or discussed with anyone other than authorized individuals. I will also violate this provision if I intentionally or negligently mishandle or destroy confidential information.
10. I understand that I am not to contact the individual(s) or other related persons to whom confidential information pertains unless I am specifically authorized to do so by law and the appropriate program manager.
11. I understand that it is a violation of Department and State of Arizona policy for me to share my sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas. I further understand that I will not use another person's sign-on code and/or password or otherwise attempt to access electronic confidential information or to gain physical access to a restricted area that is not within the scope of my work or permitted by my supervisor.
12. I understand that it is my responsibility to know and abide by any additional confidentiality provisions required by my job that may be issued by the Department, Division, Bureau, program or other work unit to which I report. If I have questions about which confidentiality rules apply to my job, I understand that it is my responsibility to ask my supervisor prior to releasing any information, even if the information request is in the form of a subpoena or other legal document.
13. I understand that it is my responsibility to report any observed or suspected breach of confidentiality by any other Department employee to my supervisor.
14. I understand that if it is determined that I have violated the Pledge or any other confidentiality requirement, I may be subject to formal disciplinary action up to and including termination of employment, loss of privileges, contractual or other rights which may be granted as a result of an affiliation in accordance with Department and/or State of Arizona procedures. Unauthorized use or release of confidential information may also subject me to personal, civil, and/or criminal liability and legal penalties.

Service Designation:

Employee Contractor Volunteer Student Other

User Signature: _____ Title: Date:

ARIZONA DEPARTMENT OF HEALTH SERVICES
DIVISION OF OPERATIONS - INFORMATION TECHNOLOGY SERVICES
ACCEPTABLE USE OF AN INFORMATION RESOURCE AGREEMENT

I, _____, have read and understand the Acceptable Use of an Information Resource policy and procedure, 1-ITS-005. I agree to comply with this policy and procedure and to protect and secure Information Resources from unauthorized or improper use. I agree to renew my Acceptable Use of an Information Resource Agreement annually. I understand that the Department reserves the right to monitor and log all activity on an Information Resource without notice. I have no expectation of privacy in the use of an Information Resource. I understand and agree that all activity conducted with an Information Resource is the property of the State of Arizona.

Authorized User Signature

Date

Authorized User Name (Print)

Authorized User Telephone

Contractor Supervisor Signature/Date

RECEIVED BY:

ADHS Use

Supervisor Signature

Date

Supervisor Name (Print)

Division

Note: An the Acceptable Use of an Information Resource Agreement will be reviewed annually on the anniversary of the authorized user's employment start date.

Distribution: Original to Information Security Officer and copies to HR Manager and Authorized User

ARIZONA DEPARTMENT OF HEALTH SERVICES		LEVEL I	SECTION	NUMBER	DATE
		I	ADHS	012-2016	08/18/16
SUBJECT:	ACCEPTABLE USE				
SUPERSEDES:	ITS005 Acceptable Use of an Information Resource				
PRIMARY RESPONSIBILITY:	Division for Planning and Operations (DPO) – Information Technology (ITS)				

PURPOSE

To outline the acceptable use of ADHS information system assets to reduce the risks to ADHS information systems due to disclosure, modification, or disruption, whether intentional or accidental.

POLICY

A. Access Agreements - ADHS Director, or designee, will ensure that individuals requiring access to organizational information and ADHS information systems acknowledge and accept appropriate access agreements (prior to being granted access) and will review and, if necessary, update the access agreements annually. [NIST 800-53 PS-6] [PCI DSS 12.3].

1. **Assign Responsibility to Provide Policy** - ADHS Director, or designee, will assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.
2. **Assign Responsibility to Keep Records** - ADHS Director, or designee, will assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

B. Access Agreement Contents - The access agreements will contain the following policy sections and statements:

1. **Expected Behaviors** - The following behaviors will be required:

a. **Practice Safe Computing** - Those accessing ADHS information systems will use caution and exercise good security practices to ensure the protection of ADHS information systems and data, including, but not limited to:

- **Opening Attachments or Links** - Use caution when opening email attachments or following hypertext links received from unknown senders.
- **Keep Passwords Secure** - Select strong passwords, do not write them down, change them frequently, and do not share them with anyone.
- **Keep Desk and Workstation Secure** - Use available operating system functions to lock the workstation when away from the desk. At the end of the day, log out of the computer, but leave the equipment powered on.
- **Challenge Unauthorized Personnel** - Assist in enforcing physical access controls by challenging unauthorized personnel who may not be following procedures for visitor sign-in, appropriate badge use, escort control, and/or entry.
- **Report Security or Privacy Weaknesses or Violations** - Report any weaknesses in computer security or data privacy, suspicious behavior of others and any incidents of possible misuse or violation of this policy to the proper authorities.
- **Wear Issued Badges** – All ADHS employees and contractors are required to wear their ADHS-issued ID badges, while in ADHS buildings, at all times.
- **Protect Confidential Information** - Confidential information will be protected in accordance with applicable statutes, rules, policies, standards, and procedures. Those accessing ADHS information systems will protect confidential information in accordance with the statewide policy 8110, Data Classification and Handling. Specifically, the following:
 - **Marking of Confidential Information** - All non-public data should be marked (labeled) as Confidential.
 - **Unencrypted Confidential Information** - Confidential information sent over email or other electronic messaging without adequate encryption will be prohibited (even to an authorized user).
 - **Storage of Confidential Information** - Confidential information must be stored in accordance with the statewide policy 8250, Media Protection.
 - **Electronic Transmission of Confidential Information** - Confidential information that is transmitted outside of ADHS information systems or on any medium that can be accessed by authorized users will be encrypted through link or end-to-end encryption with an encryption algorithm and key length that meets the Statewide Standard 8350, System and Communication Protection.

2. Prohibited Behaviors -The following behaviors will be prohibited:

- **Computer Tampering** - Unauthorized access, interception, modification or destruction of any computer, computer system, ADHS information system, computer programs or data; [ARS 13-2316.1-2]
 - **Use of Unauthorized Computing Equipment** - Installation or connection of any computing equipment not provided or authorized by management to ADHS information systems;
 - **Use of Unauthorized Software** - Installation or use of any unauthorized software, including but not limited to security testing, monitoring, encryption, or “hacking” software on ADHS computing resources; [NIST 800 53 CM-11]
 - **Unauthorized Use of Software or Services** - Use of peer-to-peer file sharing technology used for the unauthorized distribution, display, performance, or reproduction of copyrighted work; [NIST 800 53 CM-10]
 - **Introduction of Malware** - Knowingly introducing a computer contaminant into any computer, computer system or ADHS information system; [ARS 13-2316.3]
 - **System Disruption** - Recklessly disrupting or causing the disruption of a computer, computer system or ADHS information system; [ARS 13-2316.4]
 - **Circumvention of Security Controls** - Disabling software, modifying configurations, or otherwise circumventing security controls. [ARS 13-2316] Tampering with physical security measures (e.g., locks, cameras) is also prohibited;
 - **False Identity** - Falsifying identification information or routing information so as to obscure the origins or the identity of the sender, or using or assuming any information system or application identification other than your own;
- b. Unauthorized Inappropriate or Unlawful Material** - The unauthorized storage, transmission, or viewing of any pornography or other offensive, intimidating, hostile or otherwise illegal material is forbidden. Except to the extent required in conjunction with a bona fide ADHS approved research project or other ADHS approved undertaking, an employee of ADHS will not knowingly use ADHS owned or ADHS leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sex acts; [ARS 38-448] [ARS 13-2316.5]
- c. Unauthorized Use of Electronic Messaging** - The following use of electronic messaging will be prohibited:
- **Spam** - Sending of unsolicited commercial emails/electronic messages in bulk (identical content to multiple recipients).
 - **Chain Letters** - Creating of forwarding chain letters of pyramid schemes.
 - **Unprofessional Communications** - Unprofessional or un-businesslike in appearance or content.
 - **Alter Message Content** - Modification or deletion of email/electronic messages originating from another person or computer with the intent to deceive.
 - **False Identity** - Falsifying email/electronic message headers or routing information so as to obscure the origins of the email/electronic message or the identity of the sender, also known as spoofing.
 - **Mask Identity** - Unauthorized use of anonymous addresses for sending and receiving email/electronic messages.
 - **Auto-Forward to External Accounts** - Automatically forwarding email/electronic messages sent to an ADHS account to external email/electronic messages without authorization.
 - **Non-ADHS Email Accounts** - Unauthorized use of a non-ADHS email account for ADHS business.
 - **Unencrypted Confidential Information** - Confidential information sent over email or other electronic messaging without adequate encryption (even to an authorized user).
 - **Misrepresentation of ADHS** - Presenting viewpoints or positions not held by the ADHS as those of the ADHS or attributing them to ADHS.
- d. Personal Use of ADHS Information Systems** – Personal use of an information system resource is permitted as long as such use is consistent with the ADHS policies and procedures and only when all of the following conditions are met: no additional cost or expense to the State is incurred; there is no negative impact on the authorized user’s job performance; there is no negative impact on another authorized user’s job performance; there is no discredit or embarrassment to the State; and Use of an Information Resource is not for a prohibited purpose.
- e. Violation of Intellectual Property Laws** - Unauthorized receipt, use or distribution of unlicensed software, copyrighted materials, or communications of proprietary information or trade secrets.

- f. **Unauthorized Access of Confidential Information** - Unauthorized access of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The Confidentiality of information is protected by law. The unauthorized access of any confidential information is prohibited. [ARS 13-2316.07]
 - g. **Unauthorized Release of Confidential Information** - Disclosure of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The Confidentiality of information is protected by law. The unauthorized release or disclosure of any confidential information is prohibited. [ARS 36-342] [ARS 36-666] [ARS 41-151.12] [ARS 41-1750.01]
 - h. **Unauthorized Posting of ADHS Documents** - Unauthorized posting of ADHS draft or final ADHS documents is prohibited.
3. **Notifications and Acknowledgements** - The following notifications and acknowledgements will be used to inform those granted access to organizational information and/or ADHS information systems of steps ADHS may take to ensure the security of ADHS information systems:
- a. **User Responsibility Acknowledgement** - All users review and acknowledge their understanding of this policy and other related information security policies on an annual basis; [PCI DSS 12.6.2]
 - b. **Assets and Intellectual Property** - All ADHS information system assets remain the sole property of the State of Arizona. Any data or intellectual property created by the user, including voicemail and electronic messages, will remain the property of the State of Arizona and will not be removed, copied or shared with any person or entity except as part of the user's normal job responsibilities;
 - c. **Monitoring** - ADHS will inform all users that it reserves the right to monitor all activities that occur on ADHS information systems or to access any data residing on its systems or assets at any time without further notice. ADHS will retain the right to override an individual's passwords and/or codes to facilitate access by the ADHS;
 - d. **Potential Blocking of Inappropriate Content** - ADHS may block access to web content it deems as inappropriate or filter email destined for your mailbox;
 - e. **Incomplete Blocking of Inappropriate Content** - ADHS will not be responsible for material viewed or downloaded by users from the Internet or messages delivered to a user's mailbox. Users are cautioned that many Internet pages and emails include offensive, sexually explicit, and inappropriate material. Even though ADHS intends to filter and block inappropriate content and messages it is not possible to always avoid contact with offensive content on the Internet or in your email. If such an action occurs users are expected to delete the offensive material, leave the offensive site and contact the ADHS Information Security department;
 - f. **Records Retention** - Files, emails, attachments and other records are retained, preserved, and/or disposed of in accordance with ADHS record retention policies and in full accordance with the Arizona State Library Records Retention Schedule, Electronic Communication Records:
http://apps.azlibrary.gov/records/general_rs/Electronic%20Communications,%20Social%20Networking%20&%20Website.pdf;
 - g. **No Expectation of Privacy** - Users will have no expectation of privacy for any communication or data created, stored, sent, or received on ADHS information systems and assets; and
 - h. **User Acknowledgement** - By using ADHS information systems, users will acknowledge that they explicitly consent to the monitoring of such use and the right of ADHS to conduct such monitoring.
- C. **Remote Access Agreement** - ADHS will ensure that individuals utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home) to access ADHS information systems as a trusted user and to acknowledge and accept appropriate access agreements prior to being granted access and will review, and if necessary, update agreements annually.
- D. **Remote Access Agreement Contents** - The Remote Access agreements will contain the following additional policy sections and statements:
- 1. (P) **Allowable Computing Devices** - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home) to access ADHS information systems as a trusted user providing and storing confidential information will ensure:
 - a. The computing equipment is issued to the individual by ADHS for the purposes of connecting to an ADHS information system; or
 - b. The computing equipment is owned or otherwise under the control of the individual such that the individual may ensure minimum physical and logical protections are in place. Confidential information cannot be stored on personally owned equipment.

2. (P) **Physical Protection of Computing Devices** - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home) to access ADHS information systems as a trusted user providing and **storing confidential information will** ensure that computer equipment is:
 - a. Physically protected from unauthorized use and removal; and
 - b. Limited to the use of the authorized remote user. Use of the computer equipment by anyone else (e.g., family members, roommates) is strictly forbidden while device is being used for remote access.
 3. (P) **Logical Protection of Computing Devices** - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access ADHS information systems as a trusted user providing and storing Confidential information will ensure that computer equipment has the following logical security controls:
 - a. **Username and Passwords** - Identification and authentication controls consistent with statewide policy 8340, Identification and Authentication;
 - b. **Anti-Virus** - Malicious code protection consistent with statewide policy 8220, System Security Maintenance, with the exception of central management of malicious code protection;
 - c. **Personal Firewalls** - Personal firewalls consistent with statewide policy 8320, Access Control;
 - d. **Device Encryption** - Full Device Encryption consistent with the statewide policy 8320, Access Control Policy; and
 - e. **Security Patches** - Install security-relevant software and firmware updates consistent with statewide policy 8220, System Security Maintenance.
- E. **Remote Access** - Remote office users may access the ADHS information system only by approved access methods.
- F. **Mobile Technologies** – ADHS will ensure that individuals utilizing mobile technologies (e.g., smart phones, tablet computers) to access ADHS information systems as a trusted user acknowledge and accept appropriate access agreements (prior to being granted access), and will review, and if necessary, update agreements annually.
- G. **Mobile Technology Agreement Contents** - The mobile technology access agreements will be developed by ADHS and contain ADHS defined security controls according to statewide standard 8220, System Security Maintenance provides guidance to ADHS for minimum recommended mobile technology controls.
- H. **Consequences for Non-compliance** - Users of ADHS information systems who fail to comply with established information security and privacy policies and procedures may be subject to sanctions, including referral to law enforcement for appropriate action. [NIST 80053 PS-8] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)]
1. **ADHS Employees** - State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct, requires that all employees comply with federal and state laws and rules, statewide policies and employee handbook and ADHS policy and directives. As provided by SPS Rule R2-5A-501(C), an employee who fails to comply with standards of conduct requirements may be disciplined or separated from state employment.
 2. **ADHS Contractors** - ADHS contractors violating federal and state laws and rules, statewide policies, and ADHS policy and directives may result in, but not be limited to, immediate credential revocation (AD accounts or other system access), terminations of permissions for access to data systems and physical locations, and barring entry or access permanently. Vendors providing services under a contract are subject to vendor performance reports, and any contract terms and warranties, including potential damages.

APPLICABILITY

- A. **Application to ADHS** - This policy will apply to all of ADHS as defined in ARS § 41-3501(1).
- B. **Application to Systems** - This policy will apply to all ADHS information systems. Policy statements preceded by “(P)” are required for ADHS information systems categorized as Protected. Categorization of systems is defined within the statewide policy 8120, Information Security Program.
- C. **Application to End User** - The content of this policy is primarily focused towards the end-user, unless explicitly specified otherwise, as stated in Section 3.1.

ROLES AND RESPONSIBILITIES

- A. **ADHS Director or designee will:**
 1. Be responsible for the correct and thorough completion of ADHS policies, standards, and procedures (PSPs);
 2. Ensure compliance with ADHS PSPs; and
 3. Promote efforts within the ADHS to establish and maintain effective use of ADHS information systems and assets.

B. ADHS Chief Information Officer (CIO) will:

1. Work with the ADHS Director, or designee, to ensure the correct and thorough completion of ADHS Information Technology PSPs; and
2. Ensure the Acceptable Use Policy is periodically reviewed and updated to reflect changes in requirements.

C. ADHS Information Security Officer (ISO) will:

1. Advise the ADHS CIO on the completeness and adequacy of the ADHS activities and documentation provided to ensure compliance with ADHS Information Technology PSPs;
2. Ensure the development and implementation of adequate controls enforcing the ADHS PSPs;
3. Request changes and/or exceptions to existing Statewide PSPs from the State CISO; and
4. Ensure all personnel understand their responsibilities with respect to acceptable use of ADHS information systems and assets.

D. ADHS Supervisor of employees and contractors will:

1. Ensure users are appropriately trained and educated on acceptable use policies;
2. Monitor employee activities to ensure compliance; and
3. Endorse the form, acknowledging compliance with the policy.

E. System Users of ADHS information systems will:

1. Become familiar with this and related PSPs; and
2. Adhere to PSPs regarding classification of data and handling within ADHS information systems.

DEFINITIONS & ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the [ADOA-ASET website](#).

AUTHORITY & REFERENCES

Arizona Revised Statutes (ARS) § 41-3504 and § 41-3507.

Arizona Revised Statutes (ARS) § 36-104, Powers and Duties of the Director.

Statewide policy P8280, Acceptable Use

Statewide policy 8120, Information Security Program Policy

State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct

Statewide Standard 8350, System and Communication Protection

Statewide Standard 8220, System Security Maintenance

Statewide policy 8340, Identification and Authentication

Statewide policy 8320, Access Control

Statewide policy 8250, Media Protection

Statewide policy 8110, Data Classification and Handling

Statewide policy 8220, System Security Maintenance


NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013, January 2012

HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

Payment Card Industry Data Security Standard (PCI DSS) v2.0, PCI Security Standards Council, October 2010.

IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

General Records Retention Schedule for All Public Bodies, Electronic Communications, Social Networking and Website Records, Schedule Number 000-12-22, Arizona State Library, Archives and Public Records.

APPROVED: 	08/18/16
Janet Mullen, PhD, MBA Deputy Director for Planning and Operations	Date of Last Review

*** Please see the ADHS Intranet Forms & Policies Section for the most current & up-to-date Policy ***

Arizona Department of Health Services - Ryan White Part B CAREWare User Agreement

Agency: _____ Employee Name: _____

Job Title: _____ E-mail : _____

Phone: _____ Address: _____

Request Type: New CAREWare user Authorization renewal Remove User

I certify that I have received a copy of and agree to comply with the "Arizona Department of Health Services Acceptable Use of an Information Resource Agreement (ADHS Policy ITS-005)," and the Arizona Department of Health Services Confidentiality Agreement," and the "Remote Access User Responsibilities." I understand that my privileges to access CAREWare will be revoked if I violate the provisions or terms of these documents.

I understand that access to the Arizona Department of Health Services electronic-resource systems and network is offered to me solely to provide me access to CAREWare's centralized database for reporting clinical, service and demographic data as required under the Arizona Department of Health Services Ryan White Part B contract.

I further understand that CAREWare access is exclusively for my use only. I agree not to share my access credentials with anyone and agree to disallow any other person access with or to my login credentials. I agree to notify the RW Part B Program if I become aware that another person has access to my credentials or has gained unauthorized access to the Arizona Department of Health Services network.

I understand and agree that in the event I breach this agreement, my privileges under this agreement shall be revoked, and that I may be subject to penalties or liabilities under state federal law or regulations. I agree that my obligations under this agreement continue indefinitely.

I will need the following permissions granted:

View Only Data Entry Clinical Data Entry Referrals Reporting Add Client

User Signature

Date

By signing below, the user's supervisor agrees that the above mentioned CAREWare access is required by the user and agrees to monitor the user's adherence to the terms and conditions of this CAREWare/VPN User Agreement.

User's Supervisor Signature

Date

Internal Use Only

<input type="checkbox"/> CAREWare Application	_____	_____	_____
<input type="checkbox"/> CAREWare Insurance	CAREWare username	Processed by	Date Processed
<input type="checkbox"/> CAREWare Pharmacy	_____		
	Ryan White Part B Authorized Signature		



ARIZONA DEPARTMENT OF HEALTH SERVICES

PREPAREDNESS

Arizona Health Services Portal User Agreement Health and Wellness for all Arizonans

WARNING

The Arizona Health Services Portal Environment has been developed in conjunction with the statewide plan for information technology as set forth in A.R.S. § 41- 3504 (A) (1)). It is a component of the State of Arizona's Health Services Information Technology Services, which may be accessed and used only for official business by authorized personnel. Unauthorized access or use may subject violators to criminal, civil, and/or administrative action. As a State owned system, there is no right to privacy on this system. All information on this system may be monitored, intercepted, recorded, read, copied, and shared by authorized personnel for official purposes including criminal investigations

Terms of the Agreement

The terms of this Agreement shall become effective upon signature and shall remain in effect for two years after the date of signature. Arizona Health Services Portal (AHSP) users will be required to renew the AHSP Agreement on a bi-yearly basis.

Background

AHSP is a secure electronic communication system that is designed to host a series of web based applications, enabling local, state, federal, and international public health preparedness partners to share information and preliminary data on recent outbreaks and other health events in a rapid and secure environment.

Security Requirements on the Arizona Health Services Portal

- a. User will need to change password once received.
- b. User will be required to change their password every 60 days.
- c. User will be required to renew the AHSP Agreement on a bi-yearly basis.
- d. User will be limited to three (3) log-in attempts before losing access.
- e. User will need to contact the Helpdesk at helpdesk@siren.az.gov to regain access.
- f. User will notify the AHSP Helpdesk, AHSP Liaison at the Local Health Department or organization within 24 hours of any unauthorized release of personally identifying information.
- g. User will notify the AHSP Helpdesk, AHSP Liaison at the Local Health Department or organization within 24 hours of any changes in job position, responsibilities or no longer need access.
- h. User will not leave the computer unattended when logged on to the AHSP.

Agreement Provisions

The Arizona Department of Health Services Department has a duty pursuant to A.R.S. § 41-4172 to develop and establish commercially reasonable procedures to ensure the security of personal identifying information.

In consideration of the Department's duty to ensure the security of personal identifying information and my responsibilities as AHSP user, and in recognition of the potential harm or discomfort that could be caused by the release of sensitive, provisional, and personal information obtained from within the AHSP, I agree to the following provisions:

- a. To adhere to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules as defined in 45 C.F.R. Parts 160 and 164.
- b. To cooperate with the Arizona Department of Health Services in the course of performance of the Agreement so that both parties will be in compliance with HIPAA.
- c. Not to share my AHSP information (i.e. USER ID and Password) with others or to allow others to use my account to view information posted on AHSP.
- d. To use any and all information posted on the AHSP solely for the purposes of public health or emergency preparedness and not for personal or commercial gain.
- e. To avoid attempting to override or circumvent the security procedures related to the AHSP.
- f. To prohibit the use of names of other AHSP users or their institutions in a way that misrepresents the source of information or implies endorsement of products or services without the permission of the contributing source.
- g. To the use of my name and contact information in the AHSP's Public Health Directory that will be made available to all AHSP users, unless otherwise stated.



ARIZONA DEPARTMENT OF HEALTH SERVICES

PREPAREDNESS

Medical Electronic Disease Surveillance Intelligence System (MEDSIS)

- a. Only AHSP users trained by the Arizona Department of Health Services and/or a local health department representative may enter data into MEDSIS or have access to patient data in MEDSIS.
- b. MEDSIS users will comply with the Arizona Administrative Code: R9-6-201 to 207 Responsibilities for Reporting (http://www.azsos.gov/public_services/Title_09/9-06.htm). Reporting through MEDSIS fulfills most reporting requirements of communicable diseases to the local health departments. Reporting of urgent situations (such as detection of a 24-hour notifiable disease) must be done using another immediate means of communication (such as a phone call) in addition to electronic notification via MEDSIS.
- c. MEDSIS users will comply with MEDSIS Policies and Procedures regarding the release of data to non-MEDSIS persons.

Confidentiality of data on the AHSP Applications

- a. Human case information falls under HIPAA and A.R.S. §§ (36-661 to 669)
- b. Unauthorized release of confidential information will result in immediate termination of access to Arizona Health Services Portal and its applications as well as notifying your facility Administrator and/or supervisor, and may result in administrative or criminal penalties.

I have reviewed and understand the above Agreement and the MEDSIS Policies and Procedures and agree to be bound by both with regards to my access and use of AHSP and MEDSIS. Furthermore, the Arizona Department of Health Services reserves the right to limit access for violation of the above Agreement or the MEDSIS Policies and Procedures.

AHSP

PRISM

MEDSIS

Organization Name

First & Last Name (Print)

Work Phone

Work Email

Signature

Date