ARIZONA DEPARTMENT
OF HEALTH SERVICES

Division of Operations – Information Technology Services
Acceptable Use Access Agreement

I have been made aware and understand that applicable State of Arizona statutes*, rules, policies and directives bind all State of Arizona (State) employees, contractors, vendors, volunteers and other users who have access to the State's technology systems and applications.

[State of Arizona employees] This agreement does not create a contract for employment between any employee and the State. Nothing in this agreement changes the fact that all uncovered employees of the State are at-will employees and serve at the pleasure of the appointing authority.

[Non-State employees/other users (such as, contractors, leased employees, vendors, volunteers, etc).] Nothing in this agreement creates an employment relationship with the State of Arizona.

In consideration for access to State information technology systems and applications, I agree to at all times abide by all applicable Arizona State statutes, rules, policies and directives, and understand that I am prohibited from violating the foregoing, which includes, but is not limited to, the following actions:

1. Revealing data to any person or persons outside or within the agency who have not been specifically authorized to receive such data.
2. Attempting or achieving access to data not germane to my mandated job duties.
3. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts without appropriate authorization.
4. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts for direct or indirect personal gain or advantage.
5. Entering, modifying, deleting, or otherwise altering data, data structures, databases, programming code or scripts maliciously or in retribution for real or imagined abuse or for personal amusement.
6. Unauthorized access, modification or destruction of any computer, computer system, State information system, hardware appliance, network device, media device, computer program, data structure, database, or program code or script.
7. Unauthorized installation or connection of any computer or electronic equipment to a State network.
8. Recklessly disrupting or causing disruption of any computer, computer system or State information system.
9. Unauthorized use of electronic messaging or other communications.
10. Using State equipment or property, including equipment or property leased to the State, for other than work related purposes, unless authorized by written agency policy or other proper authorization.

11. Using a personal device that is not protected with approved and up-to-date anti-virus software and fully patched to access any State of Arizona network.
12. Removing sensitive data from the State network or State devices that are not fully protected with encryption.
13. Using another person's personal data access control identifier (USERID) and password.
14. Revealing my personal data access control identifier and/or password to another person.
15. Asking another user to reveal his/her personal data access control identifier and/or password.
16. Accessing, copying, disclosing, or deleting personally identifiable information, personal health information or other sensitive non-public information beyond that authorized by statute or specific authority of authorizing agent.
17. Accessing, copying, or disclosing critical information technology infrastructure information without authorization.
18. Using software on the local area network (LAN), or on any PC in any manner other than in accordance with the license agreement.
19. Making, acquiring, using, or distributing unauthorized copies of computer software.
20. Bringing in software (from outside the Agency) for use on the LAN or PC without the prior written permission of my Supervisor, Agency Authorizing Authority/Designee and unit responsible for Information Technology.

[State of Arizona employees] All new State employees must be provided with a copy of A.R.S. § 38-448 at the time of authorizing an employee to use an agency computer; the full text of this statute appears below:

38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions
A. Except to the extent required in conjunction with a bona fide, agency approved research project or other agency approved undertaking, an employee of an agency shall not knowingly use agency owned or agency leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sexual acts as defined in section 13-3501. Agency heads shall give, in writing, any agency approvals. Agency approvals are available for public inspection pursuant to section 39-121.
B. An employee who violates this section may be subject to discipline or dismissal.
C. All agencies shall immediately furnish their current employees with copies of this section. All agencies shall furnish all new employees with copies of this section at the time of authorizing an employee to use an agency computer.
D. For the purposes of this section:
1. "Agency" means:
(a) All offices, agencies, departments, boards, councils or commissions of this state.
(b) All state universities.
(c) All community college districts.
(d) All legislative agencies.
(e) All departments or agencies of the state supreme court or the court of appeals.
2. "Information infrastructure" means telecommunications, cable and computer networks and includes the internet, the world wide web, usenet, bulletin board systems, on-line systems and telephone networks.

I agree to seek clarification before entering, modifying, deleting, altering, or disclosing data. I agree to immediately notify my supervisor, manager or any member of the Agency's executive team of any suspected or confirmed unauthorized disclosure or misuse in violation of this agreement or any applicable statutes, rules or policies.

Appropriate action will be taken, including immediate termination of access, to ensure that applicable federal and state statutes, regulations and directives governing confidentiality and security are enforced. Aside from revocation of access, breach of procedures pursuant to this policy or misuse of State property including computer programs, equipment and/or data, may result in prosecution in accordance with any applicable provision of statute, including Arizona Revised Statutes (A.R.S.) Section 13-2316, for computer tampering and/or:

- [State of Arizona employees] I may be subject to discipline or separation.
- [Non-State employees/other users] Violating federal and state statutes and rules, statewide policies, and agency policy and directives may result in, but not be limited to, immediate credential revocation, terminations of permissions for access to data systems and physical locations, and barring of 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.

During all times that I have access to State information technology systems and applications, I accept responsibility for adhering to all applicable State of Arizona statutes, rules, security policies and directives and agree to abide by this agreement. I understand that I have access to instruction on and access to applicable statutes, rules and policies. Failure to accept the terms of this agreement will mean I will not be permitted access to State of Arizona produced media, data, computer equipment and software.

Print Name _____

Agency _____

Signature _____

Date _____

*Applicable State of Arizona statutes and policies include, but are not limited to:

- A.R.S. § 41-3504. Powers and duties of the department; violation; classification
- A.R.S. § 41-3507. Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure
- A.R.S. § 13-2316. Computer tampering; venue; forfeiture; classification
- A.R.S. § 41-151.12. Records; records management; powers and duties of director; fees; records services fund
- A.R.S. § 41-1750.01. National crime prevention and privacy compact
- [State of Arizona employees] A.R.S. § 38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions
- ADHS policy 8280: Acceptable Use

ARIZONA DEPARTMENT OF HEALTH SERVICES

Confidentiality Agreement Form

PLEDGE TO PROTECT CONFIDENTIAL 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 in 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.)

Revised: 02/04/15

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 manger 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 individuals(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 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 this 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 _____

_____	_____	_____
Signature	Title	Date

ARIZONA DEPARTMENT OF HEALTH SERVICES

PREPAREDNESS

Arizona Health Services Portal User Agreement

WARNING

The Arizona Health Services Portal (AHSP) environment has been developed in conjunction with the statewide plan for information technology as set forth in A.R.S. § 18-104(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 (AHSP Agreement) shall become effective upon signature. 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 90 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@azdhs.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 has a duty pursuant to A.R.S. § 18-522 to develop and establish commercially reasonable procedures to ensure that personal identifying information that is collected or obtained is secure and cannot be accessed, viewed, or acquired unless authorized by law.

In consideration of the Department's duty to ensure the security of personal identifying information and my responsibilities as an AHSP user, and in recognition of the potential harm 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 the extent applicable, 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 AHSP Agreement so that both parties will be in compliance with HIPAA, to the extent applicable.
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 any other purpose.
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.

Medical Electronic Disease Surveillance Intelligence System (MEDSIS) & Patient Reporting Investigation Surveillance Manager (PRISM)

a. Only AHSP users trained by the Arizona Department of Health Services and/or a local health department representative may enter data into MEDSIS and/or PRISM or have access to patient data in MEDSIS and/or PRISM.
b. MEDSIS/PRISM users will comply with the Arizona Administrative Code: R9-6-201 to 207 Responsibilities for Reporting (https://apps.azsos.gov/public_services/Title_09/9-06.pdf). Reporting through MEDSIS and PRISM fulfill 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.
d. PRISM users will comply with PRISM Policies and Procedures regarding the release of data to non-PRISM persons.

Sara Alert

a. Only AHSP users trained by the Arizona Department of Health Services and/or a local health department representative may enter data into Sara Alert or have access to data in Sara Alert.
b. Sara Alert users will comply with all security and confidentiality requirements outlined in this AHSP Agreement.
c. Sara Alert users will comply with MEDSIS Policies and Procedures, including but not limited to the release of data.
d. **NOTE**: Users only requesting Sara Alert access can send a completed ADHS Acceptable Use Access Agreement, ADHS Confidentiality Agreement Form, and this AHSP Agreement directly to contacttracing@azdhs.gov.

Confidentiality of data on the AHSP Applications and Sara Alert

a. Communicable disease information in ASHP falls under Arizona Revised Statutes Title 36, Chapter 6, Article 4 and is confidential pursuant to A.R.S. §§ 36-664 and may also fall under privacy protections found in the HIPAA.
b. Unauthorized release of confidential information will result in immediate termination of access to the Arizona Health Services Portal and its applications as well as notifying your facility Administrator and/or supervisor, and may result in civil, administrative, and/or criminal penalties.

I have reviewed and understand the above Agreement and the MEDSIS Policies and Procedures, including the policies and procedures related to Sara Alert (if applicable), and agree to be bound by both with regards to my access and use of AHSP, MEDSIS and Sara Alert. Furthermore, the Arizona Department of Health Services reserves the right to limit or terminate access for violation of the above Agreement or the MEDSIS Policies and Procedures.

☐ AHSP ☐ PRISM ☐ MEDSIS ☐ Sara Alert

Organization Name

First & Last Name (Print) Work Phone

Work Email

Signature Date