US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/10/2020

OPDIV:

NIH

Name:

AtHoc

PIA Unique Identifier:
P-4329189-917356

The subject of this PIA is which of the following?
Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.
Operations and Maintenance

Is this a FISMA-Reportable system?
No

Does the system include a Website or online application available to and for the use of the general public?
Yes

Identify the operator.
Contractor

Is this a new or existing system?
New

Does the system have Security Authorization (SA)?
Yes

Describe the purpose of the system.

The AtHoc is a FedRAMP authorized commercial-off-the-shelf (COTS) solution that transforms an organization’s Internet Protocol (IP) network into a comprehensive two-way emergency notification system. Each Institute/Center/Office (ICO) has the ability to send emergency messages to their staff with a NIH Enterprise Directory (NED) account. The Division of Emergency Management (DEM) staff have the ability to send messages to all NIH staff.

Describe the type of information the system will collect, maintain (store), or share.

The AtHoc system will collect, maintain (store), or share name, e-mail, work phone, and cell phone. The information that AtHoc stores is limited to what is available in NED. AtHoc also stores employee's submitted alert responses. There are three potential responses gauging an employee's current health status.

The AtHoc uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The AtHoc is a FedRAMP authorized COTS solution that transforms an organization’s IP network into a comprehensive two-way emergency notification system. Each ICO has the ability to send emergency messages to their staff with a NED account. The DEM staff have the ability to send messages to all NIH staff.

The AtHoc system will collect, maintain (store), or share name, e-mail, work phone, and cell phone. The information that AtHoc stores is limited to what is available in NED. AtHoc also stores employee's submitted alert responses. There are three potential responses gauging an employee's current health status.

The AtHoc uses specific login information to assign permissions/user roles which is considered PII. However, this is done by using the NIH Identity, Credential, and Access Management Services: IMS, which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Phone Numbers

Health status option

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Personally Identifiable Information (PII) is used so that staff can receive an e-mail, phone call, or text message about an emergency condition impacting their workplace.

Describe the secondary uses for which the PII will be used.

The secondary use of the PII is for the pilot COVID self-assessment survey where some health information is collected to determine personnel health status when returning to work.

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 301 and 302, 44 U.S.C. 3101 and 3102, Executive Order 9397

Sec. 319 Public Health Emergency Declaration http://www.phe.gov/Preparedness/legal/Pages/phedeclaration.aspx

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

SORN 09-90-2001, Records Used for Surveillance and Study of Epidemics, Preventable Diseases

SORN 09-25-0216, Administration: NIH Electronic Directory, HHS/NIH

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

An OMB collection approval number is not needed as the system only uses the PII of federal employees for internal use only and is not needed as currently Sec. 319 Public Health Emergency Declaration http://www.phe.gov/Preparedness/legal/Pages/phedeclaration.aspx.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

NED manages the process of notification and collection of personal information. Individuals are only added upon creation of a NED record, no individuals reside in AtHoc that do not also reside in NED.

Individuals are notified during the hiring process. NED maintains its own PIA, including all legal authorities documented.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

PII that is required when using Athoc is pulled from NED. There is no opt-out option. Individuals have a right to not give their information during the hiring process. However, in doing so, they will not be able to enter into a business relationship with NIH. NED maintains its own PIA, including all legal authorities documented.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Information is pulled from NED. When major changes occur, individuals are notified via an email from NED or for individuals that work off-line, their servicing Administrative Officer (AO) reaches out to them. NED maintains its own PIA, including all legal authorities documented.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Information is pulled from NED. If an individual has concerns about how their information is being used, they may update their own NED accounts or reach out to their servicing AO. NED maintains its own PIA with legal authorities documented.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

This process is inherited from NED. The AtHoc uses Application Hosting Environment's (AHE) secured environment for protection of PII. The information system relies on the Information Technology Branch (ITB) to perform periodic audits.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Users have access to the PII in the system to send a message and create distribution lists.

Administrators:

Administrators have full access to the PII in the system to create users, send messages, and create distribution lists.

Contractors:

Third party contractors have access to the PII in the system to provide back-end support and database management.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

AtHoc has 10 operator roles based on what functions and information an individual needs to have access to in the system. A user is provided the minimum level of access to accomplish their role, however all users can view contact information that has been imported into the system.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).

Describe training system users receive (above and beyond general security and privacy awareness training).

Additional user level training is given.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

AtHoc records are maintained on-site for 1 year and 3 years off-site by Blackberry. Longer retention is authorized if needed for business use in accordance with NARA record retention schedule:

GRS 06-707, Employee Health and Safety Records; Workplace environmental monitoring and exposure records. Background data; DAA-GRS-2017-0010-0007.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative safeguards: NIH staff, including direct contractors take mandatory security and privacy training and include system security and contingency plan. Access is via least privilege through role-based access, and policies for retention and destruction of PII are in place. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices.

Physical Safeguards: Physical access to the system is controlled by security guards, employee badging, proximity cards, card readers, and security cameras. Access to the server is controlled by card readers at the server room door. There is a battery backup for power until the backup generator starts. Fire protection including sprinklers, and flooding sensors at the floor level.

Technical Controls: Technical Safeguards include restricting files using secure socket layer encryption, a two-factor authentication and role-based access controls.

Identify the publicly-available URL:

https://alerts6.athoc.com/client/auth/login?ReturnUrl=%2Fathoc-iws

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No