PENNSTATE

Will Aon Hewitt keep my personal information safe?

Privacy and security of our faculty, staff, and retirees' personal information is of utmost importance to the Penn State Office of Human Resources. Prior to engaging Aon Hewitt as our business partner in this process, Procurement Services and the University's Privacy Office thoroughly vetted the contract that was ultimately executed between our two entities.

Additionally, the program has been reviewed with several University constituencies over the past several months, including the faculty senate, staff advisory, LGBTE Commission, Academic Leadership Council, and President's Council. A committee consisting of Human Resources Representatives from University Park and the commonwealth campuses, faculty from the senate benefit committee, and office of human resources staff were charged with identifying the appropriate vendor partner to administer the program. Several vendor partners were interviewed as part of a competitive bidding process.

Please review Aon Hewitt's Security and Privacy Policy which explains how they will protect your records and keep them safe and private. To further reassure you, only Aon Hewitt employees who are working with Dependent Verification Program will have access to information. Their system has role-based access so that an employee can only see what is required to perform their role in the verification process. Background checks are completed based on an employee's level of access.

Aon Hewitt's Dependent Verification Solutions system has never had a security breach, nor have they experienced any instances of identity theft during their course of business. The Office of Civil Rights, who enforces HIPAA, has strict guidelines around personal data, and Aon Hewitt would be subject to the fines based on their findings. Additionally, the University will stand behind its employees anytime a security breach has occurred as a result of Penn State's negligence. If this ever occurred, the University would provide a credit monitoring service that has identify theft insurance included with it, free of charge, to the employee and/or family members who were impacted.

Below is further information regarding Aon Hewitt's security:

- The Dependent Verification Solutions (DVS) application is monitored by TMART for up time, Webtrends for page hits and invalid access attempts, PATROL for resource utilization, and WILEY for asp.net information.
- A security audit from a third-party vendor occurs annually. In addition, Aon Hewitt conducts an annual penetration test of all Internet-facing infrastructures; this report is available to clients.
- Networks and databases, server logs, firewall logs, database performance, and individual server performance are all monitored and documented on a regular, recurring basis. Logs for critical systems are monitored 24/7, with a defined escalation process for response to events.

- All documentation is kept in dual-keyed, secure storage facilities. Access to these keys is limited to management personnel and requires their supervision to open. Removal and return of all documents are logged. All logs are reconciled at the end of each business day. Further, there is a strict, no-tolerance policy concerning the handling of documents containing sensitive participant information. This policy includes a stipulation that all documents must remain in the physical presence of the employee who has checked the document. Data entry occurs in a clean room facility to minimize the risk of unauthorized data access. Access to the data entry room is restricted to authorized personnel wearing appropriate ID badges. All data entry user systems are specifically designed not to have floppy, USB, or other removable storage media. Cell phones, cameras, and other electronics are prohibited from being brought into the data entry facility. Physical paper, while allowed in the data entry facility, may not be removed and is destroyed once used.
- Physical records that are mailed to Aon Hewitt are destroyed onsite in their secured facility. Digital information will remain on their system due to the ongoing process for new hires and qualifying events that begins January 1, 2013.

Am I permitted to use Penn State's equipment – computer, fax, or scanner – to send my documents to Aon Hewitt?

If you choose to store information on your computer or print digital files containing personal information, it is important that you understand that there are inherent risks that could result in access to your information by unauthorized parties. You are responsible for the safety of any digital files you choose to store on your computer or print for your personal reference. Please review the terms and conditions outlining the responsibility of faculty and staff as Systems Users in policy AD20, Computer and Network Safety. You should delete any digital files that contain personal information after you are done with them.

If you utilize the scan or fax option for submitting documentation, the issue of sensitive data residing on the copiers and faxes has been addressed in the newly-updated policy BS15. This policy requires anyone decommissioning a fax/scan or copy machine to take appropriate security measures. The hard drive may be removed and securely retained or destroyed or wiped to DoD/FBI standards or degaussed before the machine may be returned to the leaser or given to salvage.

The security of the machine IP address is the responsibility of the unit in which a copier/fax/scanner is maintained. The minimum standard is the purview of Security Operations and Services.

It's important that you don't send the original documents, because Aon Hewitt will destroy all documents when the verification program is complete. Black out social security numbers, monetary amounts, and account numbers on the copies.

Please call Aon Hewitt toll-free at 1-888-223-3338 with any questions or concerns.