



Adapted PRIVACY IMPACT ASSESSMENT (Adp-PIA)

Third-Party Website or Application Name:

Clinical Scheduling Web Service Application (Amion Enterprises)

DoD Component Name:

US Army Medical Command - Defense Health Programs (DHP) Funded Web Service

This Adapted PIA (Adp-PIA) Form 2930A is to be used when personally identifiable information (PII) is likely to become available via a third-party website or application (such as Facebook and YouTube). Refer to the Appendix for the definition of third-party websites or applications.

This Adapted PIA (Adp-PIA) is intended to support the management of risk to privacy. If it is likely that personally identifiable information (PII) will become available via a third-party website or application, complete this form.

(1) Describe the specific purpose of the DoD Component's use of the third-party website or application.

The Spiral Software Amion Enterprise is an application, part client-based and part Internet-based, that provides resident and staff rotation, call, shift and clinic scheduling. It meets current Accreditation Council for Graduate Medical Education (ACGME) Residency Review Committee requirements for visibility of both staff and resident on call as well as rapid communication via pager, text, e-mail or cell phone from the application. No other available single application has these capabilities and this application is in use at most major academic medical centers. Every employee has to be scheduled for work, especially the student personnel (i.e., residents) whose hours must be rigidly tracked in order to be in compliance with mandatory hour limits for providers in a resident status. Amion builds physician schedules and streamlines access to schedules and paging across the entire hospital.

(2) Describe any personally identifiable information (PII) that is likely to become available to the DoD Component through public use of the third-party website or application.

The PII collected and stored includes the last and first name or the individual's initials. Additionally, the system will list the individual's government e-mail address and telephone numbers. There is an option to collect personal e-mail addresses and alternate phone numbers as well. All PII is collected by the on-site administrator and entered into the client application used to generate the schedules.

The vendor provides very secure protection for the data and is culpable for any breaches by contract. Access is only granted with permission and by role to limit access to the PII. The system is fully audited. The risk of compromise is low. End users with accounts may access the schedules (read only) via user name and password. End users are only those personnel within the Madigan Healthcare System with a need to know.

The Spiral Software Privacy Policy is as follows: Spiral Software is committed to protecting our customers' privacy. We do not sell, rent or share e-mail addresses, phone lists or any schedule or customer data with third parties unless the other company is directly involved in providing core Amion services and agrees to use the data solely to deliver services to our customers. This policy is available online at: <https://www.amion.com/cgi-bin/ocs?Page=Help:169>.

(3) Describe the circumstances under which PII will likely become available on the third-party website or application.

The only users of the system will be members of the Madigan Healthcare System who are authorized access to the system. Members of the commercial vendor workforce tasked with development and maintenance may view the PII, but it will be no more than that already available to the Madigan users.

(4) With whom will the DoD Component share PII?

The DoD Component will not share PII with anyone other than the vendor personnel as stated above. There is no access to information outside of the designated users and roles.

(5) Will the DoD Component maintain PII? If yes, for how long, and under what circumstances?

The PII will be maintained only for the period of time the individual is assigned to or is in a training program in the Madigan Healthcare System. Once the individual leaves Madigan, any associated PII will be deleted.

(6) Describe the means and steps by which the DoD Component will secure PII that it uses or maintains.

Some of the security measures in place to mitigate risks include:

- The PII will be used only for the intended purpose of this application. Only personnel with a need-to-know can access the data.
- The use of firewalls, authentication, and encryption will be used to secure information processed. Vulnerability assessments are conducted to ensure data is protected.
- While data is being processed, all available security best practices are adhered to. Security controls are in place to ensure data is stored, processed, and transmitted by approved secure methods.
- Individuals who access the PII must complete Information Assurance Awareness, Privacy Act, and Health Information Portability and Accountability Act (HIPAA) training on an annual basis.

(7) Describe what other privacy risks exist and how the DoD Component will mitigate those risks.

The risks associated with the collection, use, and storage of personally identifiable information (PII) are unauthorized access and unauthorized disclosure. There are administrative, physical, and technical security safeguards in place to mitigate these risks.

(8) Will the DoD Component's activities create or modify a "system of records" under the Privacy Act? If yes, describe.

No, a "system of records" will not be created or modified. The "system of records" that covers the collection of PII in this application is A0040-66a DASG.