



**Adapted PRIVACY IMPACT ASSESSMENT (Adp-PIA)**

---

**Third-Party Website or Application Name:**

Electronic Residency Application Service (ERAS®)

**DoD Component Name:**

US Army Medical Command – Defense Health Program (DHP) Funded 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 Association of American Medical Colleges (AAMC) Electronic Residency Application Service (ERAS®) is a service that transmits the application and supporting documentation from applicants and their Designated Dean's Office to program directors. This information is used by Graduate Medical Education Selection Boards at some Army Medical Treatment Facilities when selecting individuals for graduate medical educational training programs. These training programs include internships, residencies and fellowships for physicians.

**(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.**

This website requires individuals to register for an account and submit documents that contain PII. The types of PII likely to become available to the DoD Component includes the individual's demographics, educational and employment information.

---

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

The applicants upload their PII to the third-party website. The Privacy Policy for this website is as follows:

AAMC Policies Regarding The Collection, Use, and Dissemination of Resident, Intern, Fellow, and Residency, Internship, and Fellowship Application Data:  
The AAMC recognizes its responsibility to treat with care the information it collects about individuals involved in medical education, and to respect their privacy relative to sensitive data concerning them. To meet this obligation, the Association has developed policies to prevent the exposure of truly confidential personal data without the permission of the individual involved, to limit the distribution of sensitive data to those situations which require it, and to permit distribution of non-sensitive, directory information wherever a useful purpose can be served.

Through the Electronic Residency Application Service (ERAS), we facilitate the transfer of information relevant to a residency, internship, or fellowship application to the programs to which the applicant designates the information to be sent. We retain the data entered by the applicant on their ERAS application, but hold supporting documents transmitted through ERAS for one year only for legal purposes, after which these documents are purged.

Medical schools and the National Residency Matching Program (NRMP) provide

information to us that we use to develop records on the participation of individuals in graduate medical education programs. These programs verify and update this information. Such information permits us to maintain accurate records of the number of residents and fellows and their mobility and allows programs to use the information to fulfill requirements of accrediting bodies and others.

We publish information on residents, interns, fellows, and applicants to residency, internship, and fellowship programs in the form of aggregate statistics in various AAMC studies and reports. We consider certain information about residents, interns, and fellows to be directory information, for example, the names and program level of those participating in these training programs. Except for such directory information and communications with the programs as a part of the application and record-keeping processes, we do not normally share information about residency applicants, internship applicants, fellowship applicants, residents, interns, or fellows with anyone in a way that would permit individual identification.

We allow one exception to the above-stated policy: exchanges with certifying boards, licensing bodies, and other organizations involved in medical education to ensure that credentials are attributed to the proper person. To facilitate this process, we sometimes exchange information on birth date and social security number with these organizations to accompany directory information. We conduct these exchanges on a confidential basis and in a way that prevents a permanent transfer of this information to the recipient organization.

We do not sell mailing lists, email addresses, or other contact information on residency, internship or fellowship applicants, or on residents, interns, or fellows to commercial vendors. However, we may enter into arrangements with commercial and noncommercial firms to verify that someone is a resident, intern, or fellow, in order to establish eligibility for products or services that the person has sought.

We use data submitted as part of an application to a residency, internship, or fellowship, or on residents, interns, or fellows, in analyses aimed at improving the quality of our products and services. We also use these data to support worthwhile research projects that help to inform policy in medical education. We support or conduct such research only after an independent institutional review board reviews the research proposal and establishes that the rights of these individuals are safeguarded. We share data submitted by students and graduates of osteopathic medical education programs, or by any applicant to an osteopathic residency or internship program, with the American Osteopathic Association, for their own policy analyses and research on trends in osteopathic medical education.

On occasion, we agree to support researchers outside of the Association who are interested in contacting residency, internship, or fellowship applicants, residents, interns, or fellows for the purpose of surveying them on issues that are important to medical education. We do this infrequently, and only by notifying the individual by email of the opportunities to participate in such research. We do not provide the email addresses of residency or fellowship applicants, residents, or fellows directly to these researchers. If you have any questions about these policies or procedures, please contact us at [privacy@aamc.org](mailto:privacy@aamc.org)

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

Only personnel with a need-to-know can access the data. These individuals include the Graduate Medical Selection Board members and personnel within the Graduate Medical Education Office.



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

The hard copies of the application packets are destroyed following the completion of the selection process. Some of the PII elements for the applicants selected for training will be maintained in a Provider Credentials File (PCF). The PCF contains personal information that originates during the pre-employment/accesion application period and serves as the basis of a comprehensive record that is maintained and routinely updated throughout the provider's entire period of employment with the Federal Government. The contents of this record are permanent; however, data determined to be either erroneous or inaccurate will be removed in accordance with Army regulations and local policy.

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

The use of firewalls, authentication, and encryption will be used to secure information processed. Vulnerability assessments are conducted to ensure data is protected.

---

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

The privacy risks associated with the PII collection are unauthorized access and unauthorized disclosure of PII. There are administrative, physical and technical security safeguards in place to mitigate these risks. Data will be protected and file permissions restrict access to data by authorized personnel only. Individuals with access to the data are trained in the use of and protection of PII.

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

The DoD Component activities will not create or modify a "system of records" under the Privacy Act.