



Adapted PRIVACY IMPACT ASSESSMENT (Adp-PIA)

Third-Party Website or Application Name:

Passport for Care® Web Application

DoD Component Name:

US Army Medical Command - Defense Health Program (DHP) Funded Application

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 Passport for Care® web application is an integral component of an innovative healthcare initiative headed by faculty members of Baylor College of Medicine (BCM) and Texas Children's Cancer Center that addresses the need to provide patients and survivors of chronic illnesses with increased access to their medical information and healthcare guidelines. It is an interactive Internet resource that provides the user with accurate, timely, and individualized healthcare information on a “just-in-time” basis. This Internet-based decision support system is designed for use by healthcare providers to provide long-term follow-up screening for late effects in survivors of childhood cancer. The Passport for Care application is unique in that it provides the caregiver and survivor with follow-up guidelines that are individualized based on the survivor’s treatment history. This application also serves as a repository of the patient’s treatment summary and a source of the survivor’s individualized guidelines. The healthcare provider accesses this site, updates the survivor's medical history, and provides follow-up guidelines to the patient. The patient does not access this site. The DoD Component has several agreements with BCM to provide these services. The types of personal information collected include patient demographic data and medical information (protected health information (PHI)). This PIA is a renewal of a prior PIA of the same name which was conducted using DD Form 2930 and approved 2 March 2012.

(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.

No PII will become available to the DoD Component through public use of this third-party website.

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

BCM Internet Disclaimer & Privacy Policy (URL: <https://www.bcm.edu/privacy>)

Baylor College of Medicine web sites are intended to provide general educational information about services offered by Baylor and to help users arrange more easily for those services. Information on Baylor web sites is written by faculty and staff affiliated with the College, while other information may be from sources outside of Baylor.

You assume full responsibility for using the information on BCM web sites, and understand and agree that BCM is not responsible or liable for any claim, loss, or damage resulting from its use by you or any user. While we try to keep the information on this site as accurate as possible, we disclaim any warranty, express or implied, including warranties of merchantability or fitness for a particular purpose. Baylor also does not warrant that access to the site will be error free or virus free.

reproducing any document in whole or in part is prohibited, unless prior written consent is obtained from the copyright owner.

By choosing to use the College's web sites, you acknowledge and agree to the terms of this Disclaimer and our Privacy Policy. We reserve the right to modify these terms and policies and recommend that you review them periodically.

Health Information

If you are a healthcare consumer who chooses to use the health related information on Baylor College of Medicine web sites, you should not rely on that information as professional medical advice or use it to replace any relationship with your physician or other qualified healthcare professional. Baylor College of Medicine web sites are not an attempt to practice medicine or provide specific medical advice and do not establish a doctor-patient relationship. Health-related information on Baylor College of Medicine web sites should not be used to make a diagnosis or to replace or overrule the advice of a qualified healthcare provider.

Users of BCM web sites should not rely on the information contained in any BCM web site for emergency medical treatment. Users should consult with a qualified healthcare professional for answers to specific health related questions.

Some Baylor College of Medicine web sites may allow you to enter your personal health information. Any personal health information you submit electronically to Baylor College of Medicine web sites is done so voluntarily. Baylor College of Medicine will not use or disclose your personal health information without your written consent or authorization, in accordance with applicable state and federal laws.

Privacy Policy

The privacy of our customers is important to Baylor College of Medicine. We understand that visitors to sites within the Baylor domain, bcm.edu, need to be in control of their personal information.

Therefore, the following is Baylor College of Medicine's Internet Privacy Policy:

- Your personal information is not required to visit our site. If you choose not to provide personal information, you can still visit the bcm.edu pages.
- Access to some areas of our site may require appropriate authorization. In that case, your unique user ID and password is required.
- Access to some areas of our site may require some of your personal information. In that case, this personal information will only be collected if specifically and voluntarily provided and authorized by you.
- Baylor College of Medicine may collect personally identifiable information only if specifically and voluntarily provided and authorized by you.
- Baylor College of Medicine may use third-party services or programs to collect or maintain any voluntary personal information you may choose to provide us.
- Personally identifying information collected will be used only in connection with bcm.edu, or for such purposes as are described at the point of collection.
- Some information collected is for statistical purposes only. Baylor College of Medicine performs analyses of user behavior in order to measure customer interest in the various areas of our sites.
- Baylor College of Medicine will make every reasonable effort to protect the personal information that you share with us as outlined in our Internet Security Policy.

•You do not need to have cookies* enabled to visit bcm.edu.

*Session Cookies and Persistent Cookies

A cookie is a small piece of information that is sent to your browser, along with a Web page, when you access a Web site. A cookie might track the pages you've visited, and the date when you last looked at a specific page. There are two kinds of cookies. A session cookie is a line of text that is stored temporarily in your computer's memory. Because a session cookie is never written to a drive, it is destroyed as soon as you close your browser. A persistent cookie is a more permanent line of text that gets saved by your browser to a file on your hard drive.

Baylor College of Medicine uses cookies to count the number of visitors and to improve the usability of our websites. We have set our software so that your browser will only return cookie information to the domain where the cookie originated (in this case, bcm.edu). No other site can request it. Note: Regardless of the particular uses for cookies on Baylor College of Medicine web sites, we will not share any cookie information with any third parties.

Baylor College of Medicine's Internet Security Policy:

Baylor College of Medicine takes reasonable efforts to safeguard any voluntary personal information you provide us by using physical, electronic and procedural safeguards based on industry standards and best practices.

While we may use Secure Sockets Layer (SSL) software in some cases to protect the security of your information during transmission, you should know that no data transmission over the Internet can be guaranteed absolutely secure.

Baylor College of Medicine e-mail functionality does not provide a completely secure and confidential means of communication. You should take any appropriate steps to assure yourself that your communication is protected.

Baylor College of Medicine will not obtain personally identifying information about you when you visit our site, unless you choose to provide such information.

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

The DoD Component will only share the individualized healthcare information with the intended patient and select health care providers within the medical treatment facility using this application.

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

The DoD Component will maintain the PII it receives from BCM indefinitely.

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

The DoD Component will secure the PII that it maintains by using administrative, technical, and physical safeguards.

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

The identified privacy risks are unauthorized access and unauthorized disclosure. These risks are mitigated using the security safeguards mentioned in Item (6) above. Any new privacy risks will be mitigated using similar security safeguards.

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

The DoD Component's activities will not create or modify a "system of records" under the Privacy Act. These activities are authorized in DoD SORN A0040-66b DASG.

REVIEW AND APPROVAL SIGNATURES

Public Affairs or other Point of Contact:

Signature: _____
Name: Melissa Forouhar
Title: LTC, MC, Chief, Pediatric Hematology Oncology
Organization: Madigan Army Medical Center
Work Telephone Number: 253-968-6144
DSN: 782-6144
Email Address: melissa.a.forouhar.mil@mail.mil
Date of Review: _____

Other (Optional)

Signature: _____
Name: Donald Kaye
Title: Information Assurance Manager
Organization: Information Management Division, Madigan Army Medical Center
Work Telephone Number: 253-968-3676
DSN: 782-3676
Email Address: donald.e.kaye.civ@mail.mil
Date of Review: _____

Other (Optional)

Signature:

Ashley Dale

Digitally signed by Ashley Dale
DN: cn=Ashley Dale, o=Defense Health Agency - HQ MEDCOM,
ou=HQ MEDCOM IA, email=ashley.e.dale.civ@mail.mil, c=US
Date: 2015.02.10 15:13:24 -08'00'

Name:

Ms. Ashley E. Dale

Title:

Acting Information Assurance Program Manager

Organization:

Headquarters, US Army Medical Command

Work Telephone Number: 210-834-5335

DSN:

NA

Email Address:

ashley.e.dale.civ@mail.mil

Date of Review:

Component Senior Official for Privacy (CSOP), or designee

Signature:

PETERSON.JOHN.PHILLIP.1014148
619

Digitally signed by PETERSON.JOHN.PHILLIP.1014148619
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=PETERSON.JOHN.PHILLIP.1014148619
Date: 2015.02.10 17:39:50 -06'00'

Name:

Mr. John P. Peterson

Title:

Chief, Privacy Act/Freedom of Information Act Office

Organization:

Headquarters, US Army Medical Command

Work Telephone Number: 210-221-4322

DSN:

471-4322

Email Address:

john.p.peterson.civ@mail.mil

Date of Review:

10 February 2015

Component CIO or designee (i.e., Department of the Navy CIO, Department of the Air Force CIO, etc.)

Signature

TUCKER.DAVID.W.1039797042

Digitally signed by TUCKER.DAVID.W.1039797042
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA,
cn=TUCKER.DAVID.W.1039797042
Date: 2015.02.17 15:45:59 -05'00'

Name:

For COL Beverly A. Beavers

Title:

Chief Information Officer/G6

Organization:

Office of The Surgeon General/HQ, US Army Medical Command

Work Telephone Number: 703-681-8286

DSN:

761-8286

Email Address:

beverly.a.beavers.mil@mail.mil

Date of Review:

17 February 2015

APPENDIX

Definitions.

Make PII Available - The term "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, posts, or associates PII while using the website or application. "Associate" can include activities commonly referred to as "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

Personally Identifiable Information (PII) - The term "PII," as defined in OMB Memorandum M-07-16 (Note 1) refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

Privacy Impact Assessment (PIA) - The term "PIA," which is now subject to the modifications in this Memorandum, was defined in OMB Memorandum M-03-22 (Note 2) as:

[A]n analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Third-party Websites or Applications - The term "third-party websites or applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a government entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain (Note 3). However, third-party applications can also be embedded or incorporated on an agency's official website.

Note 1: OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at: <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>.

Note 2: OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), available at: http://www.whitehouse.gov/omb/memoranda_m03-22/.

Note 3: See OMB Memorandum M-05-04, *Policies for Public Agency Websites* (Dec. 17, 2004) (identifying ".gov," ".mil," and "Fed.us" as appropriate government domains), available at: <http://www.whitehouse.gov/OMB/memoranda/fy2005/m05-04.pdf>.