



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

United Concordia Companies, Inc. (UCCI)/Highmark Information System
---

TRICARE Dental Program (TDP) / TRICARE Management Activity (TMA)
--

### **SECTION 1: IS A PIA REQUIRED?**

**a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

**b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

## SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System       New Electronic Collection
- Existing DoD Information System       Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR      Enter DITPR System Identification Number
- Yes, SIPRNET      Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes       No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes       No

If "Yes," enter Privacy Act SORN Identifier

DTMA 04

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

**Yes**

**Enter OMB Control Number**

0720-0035

**Enter Expiration Date**

01/31/2013

**No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. Chapter 55, Medical and Dental Care; 32 C.F.R. Part 199.17, TRICARE Program; 38 U.S.C. 1781, Medical care for survivors and dependents of certain veterans; 45 C.F.R. Parts 160 and 164, Health Information Portability and Accountability Act Privacy and Security Rules; and E.O. 9397 (as amended, SSN).

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The UCCI/Highmark IS includes systems that support operations and administration, and serve as the support infrastructure for selected application systems processed at UCCI. The UCCI/Highmark IS is a general support system providing office automation tools that assist UCCI personnel in carrying out TDP mission-related functions. These functions include, but are not limited to the following: administrative procedures, health care services, provider services, subcontractor tasks, and Information Technology (IT) projects.

UCCI/Highmark purchases, maintains, and operates the permanent equipment that is needed to accomplish the mission of UCCI. This includes, but is not limited to the following: file servers, workstations, laptop computers that are used as workstations, mainframes, routers, switches, cabling, and accessories.

The system serves the TDP Claims, Customer Service, and Enrollment & Billing areas. These areas process TDP members' claims, respond to TDP members' inquiries, enroll members into the TDP, and bill members for their TDP coverage.

Within the Certification and Accreditation (C&A) Boundary, there are dedicated servers, workstations, and databases for TDP information. Also within the C&A Boundary, there are servers, network devices, and the Mainframe (LPARs), which are used for both TDP and non-TDP information.

The office that owns the IT system is the UCCI/Highmark Information Systems Group, led by the Chief Information Officer and Information Assurance Officer, 120 Fifth Avenue Place, Pittsburgh, PA 15222.

The personally identifiable information (PII) about individuals collected in the system to perform these functions include name, phone number, mailing address, birth date, Social Security Number, gender, email address, military status, marital status, and (if being enrolled) spouse and child(ren) information. After an individual receives dental treatment, information about that treatment, which includes protected health information (PHI), is collected in the system.

Individuals whose PII/PHI is collected are family members of all active duty Uniformed Service Personnel and also Selected Reserve and Individual Ready Reserve (IRR) members and/or their family members.

The program name is the TRICARE Dental Program. The point of contact is the Senior Vice President, Department of Defense Programs and UCCI Program Manager, 4401 Deer Path Road, Harrisburg, PA 17110.

The system is accessed at only one site, UCCI/Highmark.

TDP has a web-site that is accessible by the public. The web site is housed in the UCCI/Highmark demilitarized zone (DMZ). The web site address is <http://www.tricare dental program.com/tdptws/home.jsp>.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy risks to the UCCI/Highmark IS include breach of confidentiality, misuse of information, and Health Information Portability and Accountability Act (HIPAA) violations.

UCCI/Highmark has placed the following into use in order to safeguard privacy:

UCCI/Highmark implemented security restrictions on all desktop and laptop PCs to ensure compliance with HIPAA and DIACAP regulatory requirements. These restrictions are put into place using Guardian Edge: Encryption Plus Hard Disk (EPHD) on all laptops and Pointsec Protector on all desktops/laptops. Pointsec Protector provides a Removable Media/IO Device Manager and Removable Media Encryption. Only approved devices are capable of

being accessed and the data on the approved devices is encrypted to protect from unauthorized use if they are lost or stolen.

Further, security objectives and the mechanisms in place at UCCI/Highmark are:

- Access Control - Access Control Facility 2 (ACF2), designated access rights through Virtual Telecommunications Access Method (VTAM) tables, Virtual Private Network (VPN), and review of audit logs.
- Authentication – user IDs and passwords, Two Factor Authentication, Smart Cards, Tokens, Biometrics, and Host on Demand terminal emulation program (TN3270).
- Confidentiality – secure mail software Tumbleweed and encrypted messages, Secure Socket Layers (SSL), Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), and review of audit logs/error reports.
- Integrity – individuals can only access data they are approved/authorized to view, unapproved devices cannot be attached to the UCCI/Highmark IS infrastructure, data at rest is encrypted, and administrators are notified of any attacks.
- Non-Repudiation – user authentication (user IDs and passwords, Two Factor Authentication, Smart Cards, Tokens, and Biometrics), system event logging (Quest InTrust and RSA enVision, Network Logging, and Intrusion Detection [enVision, Circulose, and WhatsUpPro]), and review of audit logs.
- Security Management – segregation of duties, access request/owner approval process, data owner reviews of accesses/privileges, unique user ID and password, limited login attempts, badge-access doors/buildings, biometrics, and security guards.

UCCI/Highmark's warning banner message displays for UCCI/Highmark users only, prior to collection of data. The current Designated Approving Authority (DAA)-approved warning banner in use at UCCI is:

"This system is for the use of authorized users only. This system may be monitored to ensure proper operation, to verify authorized use and security procedures, and similar purposes. Your use of this system constitutes consent to such monitoring. Unauthorized attempts to change or copy information, to defeat or circumvent security features, or to utilize this system for other than its intended purposes are prohibited and may result in disciplinary and/or legal action."

UCCI/Highmark users and Non-UCCI/Highmark users (potential TDP enrollees) have access to the Privacy Policy and Privacy Practices via the UCCI TDP website. On this website, there are links to the Privacy Policy and Privacy Practices. These Policies state why information is collected, list individual's rights under the HIPAA, and provide ways to obtain more information on how the Military Health System (MHS) may use/disclose personal information. The links to the Polices are available for review prior to the collection of data.

Link to Privacy Policy: <http://www.tricare.mil/privacy.cfm>

Link to Committed to Protecting Your Privacy: <http://www.tricareentalprogram.com/tdptws/info/priv-protect.jsp>

The UCCI/Highmark network is classified as a Mission Assurance Category (MAC) level III, sensitive, and requires basic confidentiality, integrity, and availability levels appropriate for sensitive information (SI). The UCCI/Highmark IS meets the requirements for MAC level III and confidentiality level sensitive, as specified and defined in the DoD Instruction 8500.2.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.**

**Within the DoD Component.**

Specify.

Data is shared with TRICARE Management Activity (TMA) via the Defense Online Enrollment System (DOES)/Defense Enrollment Eligibility Reporting System (DEERS).

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

**Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

**Yes**

**No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals have the opportunity to decline to provide PII at anytime during enrollment or claims processing. This can occur by not providing the Customer Service Representative with requested PII or not including the requested PII on the enrollment or claim form. If individuals do not provide the requested PII, it may delay or prevent enrollment in the TDP or processing/payment of their claims.

(2) If "No," state the reason why individuals cannot object.

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

**Yes**

**No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

PII/PHI created, received, maintained, or transmitted by UCCI/Highmark IS is used and disclosed of in connection with treatment, payment, and health care operations for TDP. Therefore, no consent or authorization for these uses is required under DoD 5400.11-R, DoD Privacy Program and DoD 6025.18-R, DoD Health Information Privacy Regulation.

**k. What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> <b>Privacy Act Statement</b> | <input type="checkbox"/> <b>Privacy Advisory</b> |
| <input type="checkbox"/> <b>Other</b>                            | <input type="checkbox"/> <b>None</b>             |

Describe each applicable format.

Authority: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 C.F.R. Part 199.17, TRICARE Program; 38 U.S.C. 1781, Medical care for survivors and dependents of certain veterans; 45 C.F.R. Parts 160 and 164, HIPAA Privacy and Security Rule; E.O. 9397 (as amended, SSN).

Purpose: To provide office automation tools that assist United Concordia Companies, Inc. (UCCI) personnel in carrying out TRICARE Dental Program (TDP) mission-related functions.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, the DoD "Blanket Routine uses" under 5 U.S.C. 552a(b)(3) apply to this collection. Information from this system may be shared with federal, state, local, or foreign government agencies, and to private business entities, including individual providers of care, on matters relating to eligibility, claims pricing and payment, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil or criminal litigation.

Disclosure: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays.