PRIVACY IMPACT ASSESSMENT (PIA)

For the

United Concordia Companies, Inc. (UCCI)/Highmark Information System
TRICARE Active Duty Dental Program (ADDP) / Defense Health Agency (DHA)

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 EDTMA 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

Enter Expiration Date

☒ **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 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended.

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 ADDP 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 administers the ADDP to all eligible active duty uniformed service members. This program began August 1, 2009, and replaced the Military Medical Support Office's (MMSO) administration of service member private sector dental care.

The ADDP provides private sector dental care to ensure dental health and deployment readiness for Active Duty Service Members (ADSMs). The ADDP provides dental care to ADSMs who are unable to receive required care from a military dental treatment facility (DTF). UCCI will coordinate an appointment for routine dental care (e.g., examinations, cleanings, fillings) within 21 calendar days of request and 28 calendar days for specialty dental care (e.g., crowns, bridges, dentures, periodontal treatment).

The ADDP provides authorized civilian dental care under two distinct components for ADSMs who are either referred from a DTF (DTF-referred) or reside and work (duty location) greater than 50 miles from a military DTF as part of the Remote Active Duty Dental Program.

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 ADDP Claims, Customer Service/Inquiries, and Grievance areas. These areas process ADDP members' claims, schedule appointments for ADDP members, respond to ADDP members' inquiries, and address ADDP members' appeals and grievances.

Within the UCCI/Highmark environment, there are dedicated servers, workstations, and databases for ADDP information. Also within the UCCI/Highmark environment, there are servers, network devices, and the Mainframe (LPARS), which are used for both ADDP and non-ADDP information.

The types of personal information about individuals collected in the system individuals include:

Personal descriptors, ID numbers, health information, and life information.

After an individual receives dental treatment, information about that treatment, which includes protected health information (PHI), is collected in the system.

The UCCI/Highmark Information System (IS) is a non-DoD IS. It is not owned, used, or operated by the DoD and is not used or operated by a contractor or other non-DoD entity exclusively on behalf of the DoD. The UCCI/Highmark Information System is owned and operated by Highmark and processes Sensitive But Unclassified (SBU) DoD information. The program name is the Active Duty Dental Program. UCCI's DoD Dental Programs-Operations Vice President is the UCCI/Highmark point of contact for ADDP.

(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, DIACAP, and NIST regulatory requirements. These restrictions are put into place using McAfee Endpoint Encryption Agent on all laptops and Check Point Endpoint Security on all desktops/laptops. Check Point Endpoint Security 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, a type of emulator that provides 3270 emulation).

- Confidentiality – ZixMail for encrypting email, 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 (Splunk) network logging/monitoring (NetCool), Intrusion Detection, 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 devices display the following banner prior to the collection of data:

"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 (Service Members) have access to the Privacy Policy and Privacy Practices via the UCCI ADDP website. On this website, there are links to the Privacy Policy and Privacy Practices. These Policies state how federal privacy and security laws and DoD regulations and guidelines are complied with, list individual's rights under 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/tma/privacy/
Link to Committed to Protecting Your Privacy: https://secure.addp-ucci.com/ddpddw/info/priv-practices.xhtml

UCCI/Highmark's National Institute of Standards and Technology (NIST) Certification was acknowledged in January 2014 by DHA, recognizing compliance with NIST Special Publication (SP) 800-53.

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 Defense Health Agency (DHA) via the Defense Online Enrollment System (DOES)/Defense Enrollment Eligibility Reporting System (DEERS). Data is also shared with Military Branch Headquarters and Dental Treatment Facilities.

☐ **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. Data is shared with Commercial Providers/Civilian Dentists when Active Duty Service Members are unable to receive required care from a military Dental Treatment Facility.

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 claims processing or an inquiry. This can occur by not providing the Customer Service Representative with requested PII or not including the requested PII on the claim form. If individuals do not provide the requested PII, it may delay or prevent processing/payment of their claims or the inability of a Customer Service Representative to respond to an inquiry.

(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 ADDP. 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.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

This statement serves to inform you of the purpose for collecting personal information required by the Active Duty Dental Program and how it will be used.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect your information in order to process claims, schedule appointments, respond to inquiries, and address appeals and grievances.

ROUTINE USES: Your records may be disclosed to investigate waste, fraud, abuse, security, and privacy concerns. Use and disclosure of your records outside of DoD may also occur in accordance with the DoD Blanket Routine Uses published at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a (b)).

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may delay or prevent processing/payment of your claim(s) or the inability to respond to your inquiry.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.