Privacy Impact Assessment
for the

Health Unit Medical Information System (HUMIS)

December 27, 2007

Contact Point
Office of Information Systems
Drug Enforcement Administration
202-307-1000

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878

Introduction

The Office of Human Resources, Health Services Unit (HREH) within the Drug Enforcement Administration (DEA) is responsible for tracking and managing physical examinations for DEA special agents, laboratory personnel (including forensic chemists), Special Operations personnel and special agent, diversion and chemist applicants. The Health Unit Medical Information System (HUMIS) collects and stores this data.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Health Unit Medical Information System (HUMIS) collects and stores personally identifiable information for DEA personnel and special agent, diversion and chemist applicants. The information collected from these applicants includes the applicant's last name, first name, middle initial, SSN, date of birth, addresses and phone numbers. In addition, the applicant's exam information is stored, including: the applicant’s SSN, the name of the healthcare provider who conducted the exam, and the initials of the reviewing DEA HQ physician. For DEA Personnel who fall under the periodic examination program, medical surveillance information is obtained from their periodic medical examinations (exam date, received date, doctor’s review date, medically cleared, missing information or not medically cleared).

1.2 From whom is the information collected?

HUMIS information is collected directly from DEA applicants and personnel. This includes: contracted medical providers, DEA special agents, laboratory personnel (including forensic chemists), Special Operations personnel, and special agent applicants.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

HUMIS collects personal information and medical information on applicants and employees to determine their medical clearance for the positions of special agent, diversion investigator or chemist. This information is used to ensure that those employees who are under medical requirements continue to meet their physical standards for continued employment in that series.

HUMIS uses SSN for two purposes: to query individuals and to identify/track the location of individuals within the system. Pertaining to location, HUMIS receives an NFC upload, which is a file that contains records with the SSN and definitive location of HUMIS users. HUMIS uses the SSN of current individuals within the system to match against a corresponding SSN in an NFC record and extracts the location from the NFC record to update an individual's location in HUMIS. Thus, SSN serves as a link between HUMIS and NFC. Both the query and update (identify/track) functions could be performed using first and last names, but SSN is currently the best way to ensure that the correct person is being queried and being updated with the correct location. DEA utilizes this information in order to determine the cost towards the agency's medical expenses.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

HUMIS information is used to determine whether DEA employees and applicants are medically cleared. Such information is internal to the DEA. The system is also used to determine budgetary needs. For instance, the system contains a report that indicates how many

individuals will require a medical examination within a fiscal year and, therefore, helps determine the agency's medical expenses.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

None. The information is internal to the DEA only.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

None. The information is not shared externally.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Applicants may decline to provide information, but their declination will disqualify them from employment. Employees are required to provide the requested information or face disciplinary action.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Yes, employees and applicants may consent in writing to the release of information outside DEA.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Threat: Unauthorized Access to the HUMIS system

Risk: Low

Mitigation / Countermeasures:

Authentication controls. Initial access to the HUMIS online system is limited to authorized users with active HUMIS accounts on a closed Sensitive But Unclassified (SBU) local area network (LAN) called Firebird. Multi-layered security is in effect by virtue of the fact that users must first logon to Firebird and then access HUMIS after a successful Firebird authentication. An unauthorized user would have to have knowledge of both userID/password combinations in order to gain access to HUMIS.

Role-based access controls. HUMIS is intended to be used by HREH staff. Within the application environment, the following types of users and their level of access have been defined:

Regular User: Can only see records in their group and can only forward documents to their supervisor.

Super User: Has full access to all records.

System Administrator: The designated DB System Administrator has full access to all records and can add new users to the system.

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Protection of audit data is provided at two levels, the Firebird servers and from within the Oracle Database. The Firebird servers operate under the Windows NT Advanced Server platform. Audit data is protected through access controls and permission assignments. No users of the HUMIS application have the capability to access audit trail and event log data. Audit data within the Oracle database is protected in a similar manner. No users of the HUMIS application have been assigned to roles that would allow access to the audit trail data. Only an authorized Oracle DBA user can access audit trail data.

HUMIS user accounts can be created, updated, enabled and disabled only by authorized administrators. In order to perform these functions, an individual must be identified as a System Administrator. The authorization shall come from the Employee Relations and Health Services Section Chief. Access to specific data is restricted by user classification (Regular User, Super User, and System Administrator) as well as by membership in specific enforcement groups.

HUMIS is hosted within the DEA's Firebird SBU LAN and Firebird is fully Certified and Accredited (C&A) according to generally accepted guidelines for C&A of systems for DOJ and re-accredited every 3 years. In addition, the system is also scrutinized annually with system self-assessments that verify and validate that the appropriate security measures are being effectively deployed.

Access to HUMIS is restricted to approved, authenticated users. Multi-layered security is ensured through approved Firebird access logon procedures, which are then interfaced with a separate logon and access protocol for HUMIS. Unauthorized access and identity theft are prevented first by Firebird logon procedures and then HUMIS userID/password combinations.

Conclusion

The Office of Human Resources, Health Services Unit (HREH) is responsible for tracking and managing physical examinations for various current DEA core employees and Laboratory personnel and special agent, diversion and chemist applicants. HREH collects information that includes last name, first name, middle initial, SSN, date of birth, addresses and phone numbers. In addition, the applicant's exam information is stored, including: the applicant's SSN, the name of the healthcare provider who conducted the exam, and the initials of the reviewing DEA HQ physician. This information is stored in the HUMIS system.

This HUMIS information is only available to designated individuals within HREH. The system employs various safeguards such as logon IDs and passwords to insure that non-designated individuals cannot access HUMIS information. The system also employs various measures to prevent such identifiable risks as identity theft and the unauthorized access of information even within DEA itself. The system uses such tools as audit trails, user classes, and user privileges to mitigate these risk factors.

Responsible Officials

_____/s/_____ _____

James D. Craig
Assistant Administrator
Chief Privacy Officer
Drug Enforcement Administration

_____/s/_____ _____

Wendy H. Goggin
Chief Counsel
Chief Privacy Official
Drug Enforcement Administration

Approval Signature Page

_____/s/_____ _____

Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice