Justice Management Division

Privacy Impact Assessment

for the

Employee Assistance Program Case Tracking System
(EAP Tracking)

Issued by:

Barbara Bush, Acting Senior Component Official for Privacy

Reviewed by: Eric Olson, Acting Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: March 22, 2012

(February 2011 DOJ PIA Form)

Introduction

The Employee Assistance Program Case Tracking System (EAP Tracking) is a case management and scheduling tool used by the JMD Employee Assistance Program Office counseling personnel to (1) facilitate general case-management activities for ongoing EAP cases, as well as to (2) produce high-level, statistical/demographic summary reports of EAP case-loads, and on-going organizational trends analysis.

The EAP Tracking system is self-contained with no connections to any other systems. The system uses a commercial-off-the-shelf application called Caseware 20/20, version 1.4.16. Caseware 20/20 was developed using a Microsoft Access database for its foundation. EAP Tracking is run on a hard-drive which is shared between two peer-to-peer workstations. The two computers (one serves as the application server and workstation, the other only as a workstation) are connected to each other by a single Linksys, Etherfast 10/100, 5-Port workgroup hub with an OmniCube KVM Switch at each workstation location for electronic isolation of the users' workstation keyboards, monitors and mice.

The counseling staff uses the EAP Tracking system to document their contacts with clients, as well as any necessary client referrals to care providers outside of DOJ. Records are maintained to document the work performed by the counselors on behalf of their clients and to chart the client's progress and participation in the EAP or community programs.

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?

The information collected is personally identifiable information (PII) along with demographic information on the EAP client and, if the client is a member of a DOJ employee's family, the employee with whom the client is associated. PII information elements include: First Name; Last Name; Home Address; Home, Cell, and Fax (home) phone numbers; Emergency Contacts; Insurance Carrier; Insurance Code; Insurance ID number. In order to generate statistical reports to analyze the EAP caseload, the system also collects various items of demographic information which may typically be considered PII but which will be dissociated from other items of PII. These include: Open/Closed status of the case file; Gender; Date of Birth (DOB); Race; Problem; Status of the Problem; Affiliated Agency; Relationship to Employee; Pay Grade; Job Title; Office Address; Office Phone and Fax (office) numbers; Marital Status; Current Medications; Client's Relationship to DOJ employee, and Doctor's Name and office phone numbers. Additionally contained in the file is job information for the employee, how the employee's job is affected by the problem, the nature of the client's problem(s), including the presented concern, the EAP counselor's assessment notes, and the entry of referrals for

further counseling support.

1.2 From whom is the information collected?

The bulk of information is collected directly from the client, who may be an employee or family member of the employee. As defined in Part 7 of DOJ Order 1200.1,[1] "family member" means an employee's spouse, life-partner or significant other; a parent of the employee or the employee's spouse; unmarried dependent child, under the age of 22 years - including adopted, recognized natural, and step-children, or foster children who lives with the employee in a parent-child relationship; and an unmarried dependent child, regardless of age, who is incapable of self-support due to mental or physical incapacity. For purposes of traumatic incident management, this definition may be extended to include other family members, in accordance with Part 7 of DOJ Order 1200.1. On occasion, information may also be collected or received from other sources, such as employee relations/labor relations counsel, the EAP client's supervisor, the EAP client's co-workers, employee bargaining units, EAP contractors, referral counseling and treatment programs or individuals, and other outside sources. In the case of drug abuse counseling, records may also be generated by the staff of the Drug-Free Workplace Program and the medical review officer.

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?

The information for EAP Tracking is collected for general support of ongoing EAP cases, by making the basic demographic and case status information available for use by EAP counselors. The EAP counseling personnel use the information to facilitate general case-management activities for ongoing EAP cases, as well as to produce high-level, statistical/demographic summary reports of EAP staff-member case-load, and on-going organizational trends analysis.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

EAP Tracking is established under the legal authorities of Executive Order 12564, 51 F.R. 32889; 5 U.S.C. § 3301; 5 U.S.C. §§ 7361, 7362; 5 U.S.C. §§ 7901, 7904; 42 U.S.C. §§ 290dd, 290dd-2; 44 U.S.C. § 3101; 5 CFR Part 792, Subpart A; 42 CFR Part 2; Sec. 503, Pub. L. 100-71, 101 Stat. 391, as amended; and DOJ Order 1200.1, Chapter 7-1.

[1] Available at http://www.justice.gov/jmd/ps/appendix1.htm#family_member.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The privacy impact assessment has identified the privacy risks to EAP Tracking data as compromise of data due to unauthorized access, theft of backup tapes or misuse by either government employees or persons outside the government that could enable a malicious user to commit identity theft, disclose sensitive personal information, damage the integrity of, or impede the availability of information. These risks are mitigated by a layered defense comprised of physical and logical security.

EAP determined that social security numbers are not necessary for EAP's purposes, so the case tracking system does not collect social security numbers. To the extent that EAP generates statistical/demographic summary reports of EAP staff member case load and ongoing organizational trends, the reports do not contain personally identifiable information, but are compiled using aggregate information only.

The EAP Tracking information outlined in paragraph 1.1 is stored on a standalone system without enterprise-network or Internet connections, making the primary risk to the stored information one of a purely physical nature. The EAP system's main application is a Commercial Off-the-Shelf Microsoft Access database tool called EAP Caseware 20/20 version 1.4.16. This application is controlled by a Microsoft Windows operating system on a Pointsec encrypted hard-drive, shared by two peer-to-peer EAP Tracking workstations. These workstations connect to the EAP Database server via a Linksys Etherfast 10/100 5-Port workgroup hub using an OmniCube KVM Switch for electronic isolation of the users' JCON Workstation keyboards, monitors and mice. The database is backed up using CDs; the removable media is stored in a GSA approved two-drawer security container with GSA approved combination lock.

The entire system is housed in two, key-locked, adjoining offices, inside an electronically keyed office area, in a government-leased building in Washington, D.C. The general office areas are only accessible through electronic keyed doorways. During business hours, all visitors are escorted by DOJ authorized personnel while in these office areas. After business hours, access to the floor requires passing through two electronic keyed doorways and presenting a security ID Badge to the security guard on-duty to reach the elevators; which themselves require a pass-key authorizing selection of any specific floor, or group of floors, to even be operated. All exterior entrances to the facility are video-monitored 24/7.

Unauthorized system access is addressed by the Pointsec hard-drive encryption software, and the inherent Windows operating system access controls. The Pointsec software is a Common Criteria EAL4 validated and FIPS 140-2 compliant encryption product which requires user authentication at system start-up. Should the number of unsuccessful validation attempts exceed a preset-limit, the system is disabled until someone with Pointsec Admin password capabilities clears the lock-out. Once the user

is authenticated, the operating system loads and its inherent Access Control features restrict unauthorized user from gaining access to individual directories and files. Unauthorized use of PII by federal employees is subject to federal prosecution.

All FISMA physical and logical security controls are implemented as mandated by FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," augmented by NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," and DOJ IT Security Standards for the system's security categorization of "LOW," as determined by FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems." Additional details of the JMD Human Resources implementation of these controls and associated risks and mitigation steps is reflected in FISMA and DOJ Order 2640.2F "Information Technology Security" mandated documentation.

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.

EAP Tracking is a case/client management system. The EAP counselors input the data. Data is updated after each appointment and when the case is closed. The EAP Tracking system serves as the working case file and official record of the EAP services provided for each case. It is used by EAP counselors to assist in managing and tracking cases, including reviewing the information in the files to ensure clients receive appropriate services. This database also provides generic reports reflecting statistical client-demographics data that are used by EAP for purposes of internal review and program evaluation. These reports provide basic information, such as the number of open cases, types and frequency of problems presented by clients, gender-distribution, marital status, and average number of sessions per client. In the instances where a client is referred to another care provider, appropriate information necessary to ensure adequate treatment of the problem and insurance accounting is hand copied to a form which is faxed to the outside provider's office then secured in the client's file or destroyed. The data is EAP casework related and cannot be released to anyone except the client and/or pursuant to the routine uses set forth in the new system of records notice (SORN) for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015 (available on the DOJ website here: http://www.justice.gov/opcl/privacyact.html), and as outlined in the Statement of Client Understanding, which has been revised to coincide with the new SORN (see Appendix A). These restrictions include those in 42 CFR Part 2, the Privacy Act, and the client/therapist privilege.

3.2 Does the system analyze data to assist users in identifying

previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No, this is not applicable as the system is not designed for data mining purposes.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The bulk of information is collected directly from clients, which helps to ensure the accuracy of information in the system. Information collected or received from outside sources is typically discussed with the client to confirm accuracy. In the course of their duties, the EAP counselors note any errors or inconsistencies in the data and correct the data manually.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The retention period is three years as determined by the NARA in General Records Schedule 1. All records are kept in a secure safe and only EAP counselors have access to such. Three years after a case is closed, or three years after the date of last contact with a client, all PII is deleted from the system, hard-copies of case information are shredded, and backup data files are overwritten per GRS 1.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

As indicated above, the bulk of information stored within EAP Tracking is collected directly from clients, and information obtained from other sources is typically discussed with clients, which helps to ensure the accuracy of the information. This information is for internal use and available to authorized users. Currently only the EAP counselors have such access. When the Information System Security Officer (ISSO) needs to make any updates to the system, it is done in the presence of the EAP counselors and the ISSO is not allowed to access any data. EAP Tracking runs on a shared hard drive between two peer-to-peer standalone workstations. EAP Tracking is self-contained and has no connections or interfaces with other systems.

In addition, the limited access to the system and the physical and logical security outlined in paragraph 2.3 above help ensure information is handled in accordance with the described uses.

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?

Information in the system is generally not shared with other Department components; however, information may be shared with the client supervisors and other components for reasons specified in the Statement of Client Understanding (see Appendix A).

4.2 For each recipient component or office, what information is shared and for what purpose?

Upon supervisor's request, the date and time the subject employee attended an appointment during duty-hours is reported for personnel time accounting verification purposes. No other information regarding a client's case is shared with internal components or persons, except as specified in the Statement of Client Understanding (see Appendix A).

4.3 How is the information transmitted or disclosed?

Information is transmitted via telephone, mail, or in person. No information is ever transmitted over any computer network outside the defined boundary of the EAP Tracking System.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The privacy risk of unauthorized disclosure of personally identifiable information to internal components of the Department is mitigated by limiting disclosure of information to the greatest extent possible such that it is only given in rare instances as outlined above. Also, limited release of information is transmitted by the most secure means possible to meet the delivery requirement – telephone for verification of time accountability information, and Registered U.S. Mail for hardcopy information transmittal.

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?

The information is not shared outside of the Department of Justice, except as permitted by the Privacy Act and consistent with the Statement of Client Understanding (see Appendix A). Also, a copy of a client's own EAP records will be released to the client or to a third party pursuant to the client's written request pursuant to the Privacy Act and in accordance with the procedures set forth in 28 C.F.R. § 16.41 and the SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015.

5.2 What information is shared and for what purpose?

Information released with the consent of the client could include any information in the EAP Tracking System. Information in the EAP Tracking System shared pursuant to routine uses would include only the information needed for the purposes of the specific routine uses relied upon. These routine uses are listed in the SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015.

5.3 How is the information transmitted or disclosed?

Should information need to be transmitted in a hardcopy format, it is sent via courier or Registered Mail directly to the authorized recipient. No information is ever transmitted over any computer network outside the defined boundary of the EAP Tracking System.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

No. Currently, EAP does not have a Memorandum of Understanding in place with outside parties with whom the data is shared. Laws that provide for the client/therapist privilege also restrict the re-disclosure of information by recipients.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

The Department of Justice does not require any type of training for users from agencies outside of DOJ prior to receiving access to the information in EAP.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

No, there are no provisions in place for auditing the recipients' use of the information. Laws that provide for the client/therapist privilege also restrict the re-disclosure of information by recipients.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The privacy risk of unauthorized disclosure of personally identifiable information is mitigated by limiting disclosure of information to the greatest extent possible such that it is only given pursuant to the routine uses set forth in the SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015, and the Statement of Client Understanding (see Appendix A), or directly to the client or those authorized by the client to receive the information. These releases are transmitted by the most secure means possible, including in person, fax, and registered mail transmittals.

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.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes, to participate in the Employee Assistance Program, the client must read and sign the EAP Statement of Client Understanding. See Appendix A. Notice is also provided to clients by the SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015.

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

Participation in EAP is voluntary. However, if an individual (client) wants to use the Employee Assistance Program, then he or she must read and sign the EAP Statement of Client Understanding (SCU) to use EAP services.

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?

Not as to the uses described in the SCU following signature by the client. However, as provided in the SCU, any other disclosures require the client's written consent.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Privacy risks associated with notice have been mitigated through the publication of the SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015, and the EAP SCU, designed to give adequate notice to the individual. See Appendix A.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Current EAP clients may seek to informally resolve any issues about their records directly with EAP personnel. All EAP clients may also request notice about or access to any EAP records pertaining to them, request an accounting of any DOJ disclosure of these records, or request amendment or correction of these records as provided in the Department's Privacy Act regulations set forth in 28 CFR subpart D, Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974 (28 C.F.R. §§ 16.40-.47). In addition, the SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015, outlines these procedures in the sections titled "Record Access Procedures" and "Contesting Record Procedures." These requests must be made by writing directly to: FOIA Contact, Justice Management Division, Department of Justice, Room 1111, 950 Pennsylvania Avenue, NW., Washington, D.C. 20530-0001 (Fax: (202) 616-6695). For the quickest possible handling, both the request letter and the envelope should be marked "Privacy Act Request." The request should include sufficient information to verify the requester's identity, including full name, current address, and date and place of birth. The requester must sign and date the request, and the signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. The request should also include a description of the records sought, the dates during which the individual was in counseling, and any other information which may assist in identifying and locating the record; a request seeking amendment or correction should also identify each particular record in question and state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment or correction desired.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Individuals are notified through the publication of the Privacy Act System of Records Notice in the Federal Register and through the notice of public rule making that preceded the promulgation of 28 C.F.R §§ 16.41-.47.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

This is not applicable because there are procedures for individuals to seek access to or amendment of their information. See section 7.1.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

The SORN for the Department of Justice Employee Assistance Program (EAP) Records, JUSTICE/DOJ-015, provides opportunities as noted in section 7.1. In some circumstances, furthermore, the Privacy Act gives individuals a right to contest certain actions taken as a result of agency reliance on information in the system.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

Only the EAP counselors have access to the system.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

No, only the EAP counselors have access to the data. All EAP counselors are DOJ employees.

8.3 Does the system use "roles" to assign privileges to users of the system?

All EAP counselors have signed the Rules of Behavior (ROB) for EAP Tracking. The EAP counselors have full system rights to add and update records. See Appendix B, EAP Tracking System Rules of Behavior (ROB).

8.4 What procedures are in place to determine which users may access the system and are they documented?

Only the EAP counselors have access to the system, and they must enter a user ID and password in order to gain access to the system. The counselors' use of the system is subject to the EAP Rules of Behavior. All EAP counselors are DOJ employees.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The only individuals who access the system are the EAP counselors (one of whom also acts as the System Administrator). EAP counselors must have rights to access the system granted by the EAP counselor with System Administration responsibilities. To further assure system security, the system's log files are checked periodically for anomalous activities.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

As previously mentioned, auditing measures in place to prevent misuse of data include the periodic review of the system's log files. Technical safeguards in place to prevent the misuse of data are the requirement of a username and password to gain access to the system and the encryption of the hard drive on which the database of employee/client information resides. In addition, the workstations are locked in two separate rooms. Backup CDs are locked in a fireproof safe in one of these locked rooms. The locked safe mitigates the risk of theft of backup CDs.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

The EAP counselors are trained on privacy of EAP data, including restrictions on disclosure based on 42 CFR Part 2, the Privacy Act and the client/therapist privilege. In addition, the EAP counselors sign the EAP Tracking Rules of Behavior and complete the annual Computer Security Awareness Training (CSAT), which the Department of Justice requires for all DOJ employees.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes, data is secured in accordance with FISMA requirements. Certification & Accreditation was last completed on 3/28/2011.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and

describe how they were mitigated.

The privacy impact assessment has identified the privacy risks as the compromise of EAP Tracking data via unauthorized access, theft of backup CDs or misuse by government employees that could enable a malicious user to commit identity theft, disclose sensitive personal information, damage the integrity of, or prevent the availability of information.

These risks are mitigated by a layered defense comprised of physical and logical security. Security guards, access badges and security cameras help ensure there is no unauthorized access to DOJ facilities. These workstations are locked in two separate rooms. Unauthorized access to the system itself is addressed by access controls, which include user id and password and role based access control and computer contaminant detection and correction software. In addition, the hard drive on which the database of employee/client information resides is encrypted. Since the system is standalone and not connected to the local area network or the Internet, it is not vulnerable to threats that exist to a system that is connected. Backup CDs are locked in a fireproof safe in one of these locked rooms, so the locked safe mitigates the risk of theft of backup CDs. Unauthorized use by a federal employee is subject to strict penalties.

Also, previously mentioned, auditing measures are in place to prevent misuse of data. This includes the periodic review of the system's log files.

Justice Management Division/Human Resources implements FISMA security controls as mandated in FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," and augmented in NIST SP 800-53, "Recommended Security Controls for Federal Information Systems." The JMD/Human Resources implementation of these controls and associated risks and mitigation is reflected in FISMA and DOJ Order 2640.2F "Information Technology Security" mandated documentation.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes, the EAP Office selected the Caseware 20/20 application after researching functionality, cost and vendor support of it and similar software applications.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your

system.

The concept of “most restrictive, least privilege” access control methods were the basis for the design and implementation of the system to assure data integrity, privacy and security through the extremely limited user-base.

9.3 What design choices were made to enhance privacy?

To enhance privacy, while still meeting the business need of the office and provide the highest possible level of security at lowest possible cost, the EAP Tracking system was designed as a stand-alone system with no connections or interfaces to other systems. Because their use was deemed unnecessary, Social Security numbers are not used in any portion of the database; further enhancing clients’ privacy.

Conclusion

The Employee Assistance Program Case Tracking System (EAP Tracking) case management and scheduling tool uses a commercial-off-the-shelf application, called Caseware 20/20, version 1.4.16. Caseware 20/20 is based on a Microsoft Access database foundation and run by two peer-to-peer workstations from a single shared hard-drive. The EAP Tracking system is fully self-contained with no connections to any other systems. It is used only by Employee Assistance Program Office counseling personnel (currently only two people) to facilitate general case-management activities for ongoing EAP cases, as well as to produce high-level, statistical/demographic summary reports. Other system support and security personnel are only allowed escorted access to the equipment for system hardware and software maintenance and security updates. Computer support and security personnel are never permitted to access client information stored in the Caseware database in any readable form. The computer Windows operating system has been configured with only user accounts for the EAP counselors.

The system is installed in a physical location with security sufficient to make undetected, unauthorized physical access to the equipment nearly impossible. Additionally, should such physical access be gained, and removal of the equipment accomplished, the use of the Pointsec PC hard-drive encryption software makes effective recovery of any readable data, extremely improbable without extensive technical capabilities.

All personally identifiable and Privacy Act-protected Information stored in the EAP Tracking system, and any products thereof, are handled and protected in accordance with applicable laws and policies, as discussed in this document and its appendices. EAP personnel understand that failure to strictly adhere to these requirements could result in severe consequences ranging from personnel disciplinary actions to federal prosecution.

Appendix A

STATEMENT OF CLIENT UNDERSTANDING

Welcome to the EAP. The EAP is a confidential, voluntary, no-cost program that provides assessment, short-term counseling, and referral services for a wide range of personal and job-related concerns. Federal laws govern the confidentiality and safe-keeping of client records. Please remember that your use of email to the EAP may compromise the confidentiality of your communications with us.

The EAP may disclose specific relevant information in certain limited circumstances as permitted under the Privacy Act, including the following:

- By your written consent.
- To contract counseling and other providers to the extent necessary to perform their duties.
- To appropriate State or local authorities to report incidents of suspected child, elder, or domestic abuse or neglect, when required by State law.
- To any appropriate person to prevent an imminent crime threatening loss of life or serious bodily injury, or when the client poses a danger to self.
- To any person to the extent necessary to meet a medical emergency.
- To law enforcement officers to report information directly related to the commission or threat of a crime on EAP premises or against EAP personnel.
- To any responsible caregiver when the client is mentally incompetent or under a legal disability.
- To qualified personnel for research, audit or program evaluation purposes.
- To report initial EAP attendance to your referring manager if you were formally referred in writing, or, when your supervisor requires confirmation that you made or kept EAP appointments during regular duty hours, including arrival and departure times. Manager/Supervisor:_____
- To a former EAP employee for purposes of responding to an official inquiry by a federal, State, or local government entity or professional licensing authority, or, to facilitate communications when the Department appropriately requires information or consultation from the former EAP employee.
- To appropriate personnel when the Department suspects or confirms: the security or confidentiality of EAP records has been compromised; there is a resulting risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of the EAP records; and, the disclosure made is reasonably necessary to respond to the compromise and prevent, minimize or remedy such harm.

I understand that authorized EAP services are free of charge. I acknowledge and understand that the Justice Management Division (JMD), its EAP contractors, and its customer organizations are not responsible for the treatment costs and/or services for which I may be referred beyond the EAP counselor or preauthorized sessions with an EAP contract provider. I understand that it is my sole responsibility to pay for all such additional services including all charges not covered by insurance plans.

I understand that if referred to a contract EAP counselor, information about my contacts with that counselor may be disclosed to the JMD EAP counselor responsible for contract quality assurance. Such information might address counseling related issues, service coordination matters, complaints and possible billing related matters. The JMD EAP will hold any such shared information in strict confidence.

I have read the foregoing Statement, and I understand and agree to it.

Client _____ _____ Date: _____
(**Print Name**) (**Signature**)

EAP Counselor _____ Date: _____

Appendix B

EAP Tracking System RULES OF BEHAVIOR (ROB)

1. OFFICIAL BUSINESS

a. Do not misuse EAP Tracking software, information, or equipment.

b. Do not use the EAP Tracking tool for non-work purposes except as approved by the Department.

2. Access

a. Only use EAP Tracking data you have been authorized to use.

b. Do not retrieve information from EAP Tracking for someone who does not have authority to access the information. Give EAP Tracking information only to people who have access authority and who need the information for their jobs.

c. Abide by procedures governing the channels for requesting and disseminating EAP Tracking information.

d. Access to EAP Tracking information and Personally Identifiable Information is only allowed for authorized EAP system users. Remote access to EAP data is not allowed.

e. Do not attempt to gain access to information to which you do not have authority.

f. Do not attempt to alter or bypass the access control/security.

g. Removal or copying of EAP data using removable media including diskette drives, CD-ROM, DVD-ROM, and USB drives is not allowed except of official EAP system back-ups. All official EAP backup media are to be stored in EAP file proof safe, located in EAP National Place Office space.

3. Integrity

a. Discontinue use of any PC system or software that show indications of being infected with a virus, and notify your security officer.

b. Protect against viruses and similar malicious programs: use only authorized software; do not use shareware, public domain software, or similar programs unless they are authorized.

c. Never enter unauthorized, inaccurate, or false information into EAP Tracking.

d. Do not manipulate EAP Tracking information inappropriately.

e. Create only authorized EAP Tracking records or files.

f. Execute virus protection on your PC according to procedures. Scan all files and disks for viruses before use, especially if they are received from external sources.

g. Keep a record of all changes made in system configurations.

h. Keep up to date hardcopy files of all active EAP cases.

4. Availability

a. Plan for EAP Tracking contingencies such as disaster recovery, loss of information, and disclosure of information by preparing alternate work strategies and recovery mechanisms.

b. Make backups of EAP Tracking systems and files on a regular, defined basis.

c. Write-protect backups.

d. Store backups away from originals.

e. Keep storage media away from devices that produce magnetic fields.
f. Keep up to date hardcopy files of all active EAP cases.

5. Hardware/Software

a. Safeguard computer equipment against waste, loss, abuse, unauthorized use, and misappropriation.
b. Use only equipment and software for which you have been granted authorization.
c. Do not store combustible materials near a computer.
d. Do not remove a PC or other computer hardware from DOJ premises without a property pass.
e. Remove computer equipment from DOJ premises for official purposes only.
f. Do not allow someone to perform maintenance without proper identification.
g. Do not install unauthorized software.

6. Reporting

Report all security violations, incidents, and vulnerabilities to the Department Security Officer. Refer to latest EAP IRP for guidance on reporting incidents.

7. Privileged Users

a. Protect the EAP Tracking supervisor's or root password at the highest level of sensitivity for the system.
b. Help train users on appropriate use and security of EAP Tracking.
c. Watch for unscheduled or unauthorized programs running on a recurring basis.
d. Track all EAP Tracking security incidents occurring within your area of responsibility.
e. Take action to reduce damage caused by security incidents, as appropriate (e.g., lock up property, log out a terminal).

8. Users of Public Access Systems

There is no public access provided to the EAP Tracking System. EAP Tracking will be accessed only from EAP Tracking workstations.

9. Managers

a. Notify security personnel whenever an employee using EAP Tracking terminates or changes status.
b. Ensure continued availability of data when a employee terminates: get passwords and user IDs, get documentation on tasks.
c. Counsel terminating employees on non-disclosure of sensitive EAP Tracking information.
d. Terminate access to EAP Tracking information and computer systems immediately in the event of an unfriendly separation.
e. Physically remove an employee when there is likelihood of sabotage, as with an unfriendly termination or separation.
f. Ensure employees get adequate and appropriate training to conduct their EAP Tracking functions.