Section I

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Medgate
Bureau: Department of Energy
Project's Unique ID: Medgate
Date: August 6, 2008

A. CONTACT INFORMATION:

1) Who is the person completing this document?
Name: Gaye Bond
Title: Technical Lead
Organization: Science Applications International
Address: P.O Box 4699, Building 1007, MS 7022
Oak Ridge, TN. 37831-7022

2) Who is the system owner?
Name: R. Burt Prater, M.D.
Title: Corporate Medical Director
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1007, MS 7422
Oak Ridge, TN. 37831-7422

3) Who is the system manager for this system or application?
Name: David D. Newton
Title: Applications Manager
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1007, MS 7022
Oak Ridge, TN. 37831-7022

4) Who is the IT Security Manager who reviewed this document?
Name: David Rose
Title: Cyber Security & Compliance Manager
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1007, MS 7022
Oak Ridge, TN. 37831-7022

5) Who is the Privacy Act Officer who reviewed this document?
Name: Amy Rothrock
Title: Privacy Act Officer
Organization: Department of Energy/Oak Ridge Operations
Address: 200 Administration Rd.
Oak Ridge, TN. 37830

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals? Yes

a. Is this information identifiable to the individual? Yes

b. Is the information about individual members of the public? Yes

c. Is the information about DOE or contractor employees? Yes

2) What is the purpose of the system/application?
The Medgate application is a COTS package that provides an integrated, secure, highly interactive method for supporting the Occupational Health at ETTP Health Services, including scheduling appointments, tracking visits, recording laboratory test results, maintaining a medical history, documenting provider information, and enrollment of patients in programs of medical surveillance.

3) What legal authority authorizes the purchase or development of this system/application?
Department of Energy

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?
Contractor and former contractor (public)

2) What are the sources of information in the system?

a. Is the source of the information from the individual or is it taken from another source?
Some data comes directly from individuals and some information comes from other applications within the boundary.

b. What Federal agencies are providing data for use in the system?
None

c. What Tribal, State and local agencies are providing data for use in the system?
None

d. From what other third party sources will data be collected?

Methodist Medical Center – lab results are loaded from an encrypted disk. The badge is used as the identifier.

e. What information will be collected from the individual and the public?
This application collects (from employees) the following:
SSN, gender, date of birth, marital status, address, phone number, spouse's name, and medical history.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?
BJC functional OH&S personnel have processes in place to ensure accuracy of the data.

b. How will data be checked for completeness?
BJC applications require a complete set of data for processing purposes. Procedures and processes are in place to ensure the completeness of the data.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?
BJC OH&S personnel have processes and procedures in place to ensure the accuracy of the data.

d. Are the data elements described in detail and documented?
No.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Yes

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? No

3) Will the new data be placed in the individual's record? N/A

4) Can the system make determinations about employees/public that would not be possible without the new data? N/A

5) How will the new data be verified for relevance and accuracy? N/A

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? N/A

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? N/A

8) How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.
Data is retrieved by Name, SSN, or Badge.

9) What kinds of reports can be produced on individuals?
Numerous business-related reports are available with information about individuals (employees and subcontractors).
Employee Hearing Summary Report (includes badge number, DOB, Sex, Name)
Duty Disposition Report
Employee Problem List Report
PHYSEXAM
MOHIS_MH
Schedule Notification Report (includes name, badge number, home address)
Schedule Recall Report (includes name, badge number)

What will be the use of these reports?
Reports are used for the business of the BJC OS&H.

Employee Hearing Summary Report (includes badge number, DOB, Sex, Name)
Used to plot the baseline hearing test against the current test for comparison to determine degree of injury.
Copy placed in chart, one may be given to the employee, one may be provided to an outside physician if the employee is sent for a hearing work injury evaluation.

Duty Disposition Report
Used to document the employee workplace duty limitations due to work related and non-work related illnesses and injuries.
Sent to employee's supervisor, employees, project safety manager, and in work related injury cases RISK management, and the Workers Compensation Insurance Adjuster.

Employee Problem List Report
Used to document the employee's emergency contact information, current medications, allergies, diagnoses, and any other information that may be needed in a medical emergency.
Kept on the 2nd page of the employee's chart.

PHYSEXAM
Used to document the physician, PA, or Nurse Practitioner's physical exam for new hire or medical surveillance to determine the employee's capability of performing the expected job duties assigned him/her at that given time.
Kept in employee's chart.

MOHIS_MH
Used to document an employee's past and current medical history in order for the practitioner to use with findings during the physical exam to determine the employee's capability of performing the expected job duties assigned him/her at that given time.
Kept in employee's chart.

Schedule Notification Report
Used by admin schedule person to pull list of names of persons needing physicals for a specific time period. Document provides contact names.
When scheduling completed document is filed in locked chart room for one year and then shredded.

Schedule Recall Report
Used by admin schedule person to pull list of names of persons needing physicals for a specific time period. Document provides contact names.
When scheduling completed document is filed in locked chart room for one year and then shredded.

Who will have access to them?
Reports are available to functional staff as needed to perform their job. The reports are printed and placed in the proper folder. All folders are located in a locked room for access to OS&H department personnel or other authorized personnel.

10) What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?
Individuals are not required to provide their home phone numbers, home addresses, social security numbers or birthdates. OS&H does not provide any additional means for individuals to decline or consent uses of the information.

E. Maintenance and Administrative Controls:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
The applications do not cross Accreditation Boundaries.

2) What are the retention periods of data in the system?
A retention period has not been noted for the system but the data is available by hard copy record for 75 years past termination per DOE policies and retention schedule.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?
Disposition of the data for the BJC D&D Contract will occur at the end of the contract. At that time, data will be turned over to DOE or designated Contractor. Data will be archived or deleted at the end of the contract based on DOE guidelines for retaining records. Currently records are maintained by the Document Management Center for 75 years after the employee is terminated and then disposed of per DOE schedule and policy. See BJC procedure BJC-OS-1001.

4) Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? No

5) How does the use of this technology affect public/employee privacy? N/A

6) Will this system provide the capability to identify, locate, and monitor individuals?
No.

7) What kinds of information are collected as a function of the monitoring of individuals?
N/A.

8) What controls will be used to prevent unauthorized monitoring?
No monitoring is possible outside of normal applications usage.

9) Under which Privacy Act system of records notice does the system operate? N/A

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? N/A

F. <u>Access to Data:</u>

1) Who will have access to the data in the system?
Access to data is controlled by the applications administrators for each application. OS&H group request access for an individual with specified roles through UCAMS.

2) How is access to the data by a user determined?
Access to data is approved by the application owners and granted by the application administrator on a need-to-know basis.

3) Will users have access to all data on the system or will the user's access be restricted?
User access is controlled by the system administrators by granting roles to individuals. Roles are restricted to see only the functionality/data required by that role.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?
Application owners enforce separation of responsibilities to only allow access to functionality/data necessary to perform job functions.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses included in their contracts and other regulatory measures addressed? Yes, DOE Privacy Act clauses are included.

6) Do other systems share data or have access to the data in the system? If yes, explain.
No.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
Any applications that process Privacy Act data are classified as "Protected" by the BJC Cyber Security Manager. Those applications then document and test the controls necessary to protect the interfaces/data.

8) Will other agencies share data or have access to the data in this system?
No.

9) How will the data be used by the other agency?
N/A.

10) Who is responsible for assuring proper use of the data?
N/A.

SIGNATURE PAGE		
	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	