Privacy Impact Assessment
for the

Medical Credentials Management System

February 10, 2011

Contact Point
Kathryn Brinsfield
Director, Workforce Health and Medical Support Division
Office of Health Affairs
202-254-6479

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Office of Health Affairs (OHA) is instituting a centralized medical credentialing system for DHS employees that provide health care services as part of their job and the Components' mission or incidental to their ongoing operations. The purpose of the program is to formalize a process for verifying DHS employee (applicant) qualifications, licensure information, and relevant health care provider data. In accordance with the DHS Directive 248-01, Medical Quality Management, the Assistant Secretary for Health Affairs and Chief Medical Officer (ASHA/CMO) is responsible for developing a centralized credentials management system for approving credentials for DHS employee medical care providers. The credentialing process will include the collection of and maintenance of information related to professional education, state license number(s), national registry certification, board certification, training and other pertinent information related to medical care practices. OHA conducted this privacy impact assessment (PIA) because the medical credentials management system will collect and maintain personally identifiable information (PII) on DHS medical care providers.

Overview

The purpose of the program is to establish a medical credentialing system within OHA for DHS employees that provide health care services as part of their job and the Components' mission or incidental to their ongoing operations. The OHA, Workforce Health and Medical Support Division will own and operate the activities of this program, to include the development of a database to input and maintain medical credentialing information on those DHS employees (applicants) requesting verification of medical credentials. The Assistant Secretary for Health Affairs and Chief Medical Officer (ASHA/CMO) as per DHS Delegation 5001 and Directive 248-01, Medical Quality Management (MQM) Program has delegated authority to exercise oversight of all medical and public health activities of DHS, and to ensure the MQM program is appropriately implemented within the Components providing health care services and consistently applied across the Department. A key element of the MQM program is the development of a centralized medical credentialing program that will formalize a process for verifying applicant qualifications and licensure information.

DHS Medical Credentialing information will be collected on a credentialing form completed by the applicant, who must be a DHS employee. The applicant completes the credentialing form to include name, duty location and provides a photocopy of current licenses, certifications, and/or registrations relevant to their individual training and status (See Appendix I, EMS or Health Care Provider Credentialing Forms). The applicant then forwards the credentialing form to his/her Component where the authorized Component official will endorse the applicant. OHA will receive the credentialing request via the OHA credentialing mailbox at ohacredentialing@hq.dhs.gov and input information into a credentialing spreadsheet and upon purchase, a secure database serving as a repository for all applicants applying to be credentialed. Although there are inherent privacy risks associated with the collection and maintenance of applicant medical credentialing information, it is essential that this information be collected in order to verify that the applicant is in good standing to practice and provide medical care for, or on behalf of DHS. OHA will verify a specific credential(s) with the identified institution or entity that

provided the credentials (Primary Source) to determine the accuracy of a qualification reported by the individual health care practitioner. For example, Emergency Medical Service (EMS) medical care providers will be verified against the National Registry of Emergency Medical Technicians (NREMT) and Registered Nurses will be verified by the respective state license agency. Additionally, all applicants will be verified against the National Practitioner Data Bank (NPDB) and Healthcare Integrity and Protection Data Bank (HIPDB) for any adverse licensure action, paid medical malpractice judgements/settlements, professional society membership actions; professional education and certifications will also be verified with other relevant agencies specific to the professional level of the applicant.

Designated OHA employees will manage all credentialing files, maintain them in a secure room and/or locked file cabinet with limited access, and ensure appropriate access controls and password protections are established and implemented in the development and implementation of a credentialing management system database. Upon verification of the DHS employee's medical credentials, the DHS medical care provider will be permitted to deliver health care services for, or on behalf of the Department.

Medical credentialing information will be maintained on all DHS health care providers until such time as the member is no longer medically credentialed under DHS, either through retirement and/or duty reassignments. Components will notify OHA via the OHA credentialing mailbox at ohacredentialing@hq.dhs.gov or by telephone regarding a health care providers change in status. In addition, OHA as part of the quality review process will review with Components status of health care providers against those identified on the spreadsheet and/or database annually. OHA will retain all historical files (either paper or electronic) on credentialed DHS medical care providers until such time as they are no longer eligible (e.g., retire, transfer or change in position) to be credentialed. OHA will follow OPM/GOVT-1 guidance for retention and disposal, items a - c for handling of both electronic and paper credentialing files. Any unauthorized access to either the paper or electronic files will be tracked by audit trails of attempted access to the system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The ASHA/CMO leads OHA and has primary responsibility within the Department for "ensuring internal and external coordination of all medical preparedness and response activities including training, exercises, and equipment support". See Section 516 (c) (3) of the Post Katrina Emergency Management and Reform Act, P.L. 109-295, 6 U.S.C. 321e(c). In addition, the Secretary has delegated to the ASHA/CMO responsibility for providing oversight for all medical and health activities of the Department, reference Delegation to the Assistant Secretary of Health Affairs and Chief Medical Officer, No. 5001 (signed July 28, 2008). As per Directive 248-01, Medical Quality Management (MQM) Program, the ASHA/CMO develops a centralized credentials management system and approves credentials for all healthcare personnel of any DHS Component.

The project will not collect Social Security numbers as part of the medical credentialing process; information collected will be relevant to medical credentialing and available to query as part of the verification process on publicly available websites designated for such purposes (e.g., NPDB/HIPDB, NREMT, State License and certification sites).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Medical credentialing information collected from eligible applicants requesting a DHS medical credential will be conducted in accordance with and under OPM/GOVT-1, General Personnel Records (71 FR 35356).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

No. Initially all relevant data elements and medical credential information for applicants will be captured in a spreadsheet until the technology solution is determined whether it be as an in-house database development or commercial-off-the-self (COTS) product. The database will reside on the OHA shared drive, with limited user access enforced by passwords that will be required to view and/or query the database files. The OHA shared drive resides on the certified and accredited unclassified local area network. Upon migration to either an in-house database or COTS product, OHA will work with OCIO and Security Compliance Office to build a System Security Plan and Certification and Accreditation of the identified system if required.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Information collected is covered under OPM/GOVT-1, General Personnel Records and retention of files will follow General Schedule 1, Civilian Personnel Files, Section 1, Official Personnel Folder (OPF) and Section 29, Training Records.

OHA will manage and retain medical credentialing files (paper and electronic) in a locked file cabinet or locked room and only those requiring access to those files will be granted access. Workforce Health and Medical Support Division will maintain a current list of members designated to have access to medical credentialing files. Electronic records are protected by restricted access to the database or equivalent system through identified OHA administrators or others with a need to know. Each user will have a protected password to view and/or query the database files.

Components will follow the same practices for securing both paper and electronic files to include any specific internal Component policy guidance.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information maintained in the medical credentialing management system is not subject to the requirements of the PRA because it pertains only to DHS employees.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Information collected on DHS employees who are health care providers includes, but is not limited to name, duty location, address, telephone number, and documents that support qualifications and other credentials (licenses, certifications and/or registrations, relevant training and experience) necessary to perform designated medical services.

In the verification process for medical credentials, OHA designated staff will make contact either by telephone or publicly available websites to verify credentials with information that was provided by the applicant (e.g., www.nremt.org provides a link to check status of nationally certified EMS professionals either by state of EMTs residence, first and last name or by individuals national registry number). Applicants' verification data will be entered into the credentialing spreadsheet and will include OHA contact working credentialing package, verification contacts, date and times, where information was verified, notation of any scanned documents received from credentialing agency(s), final determination of package (approval/disapproval), and status as a DHS health care provider. All verification information will be maintained should questions arise regarding the applicants' credentialing package (credentialing form and supporting documents).

Upon applicant verification and approval, OHA approves the DHS health care provider to deliver health care services for, or on behalf of the Department. The health care provider name, Component, license level, identification number, additional permitted skills (list), DHS provider effective date and expiration date will be entered into the centralized medical credentials spreadsheet and/or database for tracking.

2.2 What are the sources of the information and how is the information collected for the project?

The DHS employee will submit a completed credentialing form and request for consideration as a DHS health care provider and will include supporting documents related to medical credentials. Information submitted to OHA will be entered into a credentialing database for internal use by OHA only. As part of the medical credentialing process, OHA will verify the applicants' professional background and licensing information through publicly available web-sites. The areas include, but not limited to: direct correspondence, telephone verification, reports from professional organizations and public web-

site verification (medical education, board certifications, state medical licenses for physicians, National Council of State Boards of Nursing, National Registry of Emergency Medical Technicians (NREMT); Department of Health and Human Services, National Practitioner Data Bank (NPDB) and Healthcare Integrity and Protection Data Bank (HIPDB); Department of Justice, Drug Enforcement Administration (DEA) for licensing, registered to dispense controlled substance in the course of professional practice). As part of the credentialing process it is essential for OHA to exercise primary source verification to ensure that the applicant is in good standing to practice within their scope and adheres to applicable federal, state and professional agencies/organizations requirements and standards.

Information collected will be used solely for purposes of verification (either in writing or by phone) to the respective professional body(s) prior to approval as a DHS health care provider.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

As discussed in 2.2, publicly available data is used to verify professional medical background and licensing information. In accordance with DHS Instruction 248-01-001, Medical Quality Management, Item VI, Section O, Credentialing Process, the applicant in request of a DHS medical credential provides OHA with the information knowing that specific references will be verified to ensure legitimacy of the employee and that they are in good standing within their respective profession and medical practice. By signing the credentialing form, the DHS employee (applicant) consents to and as noted, "understands that all information on this application is correct to the best of my knowledge and is subject to verification" and as noted under the Privacy Act Statement which addresses the authority, purpose, routine uses as per OPM/GOVT-1, General Personnel Records, and disclosure of how information will be utilized.

2.4 Discuss how accuracy of the data is ensured.

The DHS Employee who is applying to be a DHS credentialed health care provider will submit medical credentialing information on the credentialing form through the DHS Component. OHA will utilize the applicant credentialing information to conduct license, certification and/or registration verification. Any discrepancies noted would be based on the applicant providing inaccurate information on the form or potential of the license, certification and/or registration agency having incorrect information. If unable to complete the verification process, OHA will refer back to the applicant and request that they correct information with the respective agency and subsequently resubmit updated information back to OHA. For OHA to ensure accuracy when transcribing information into the database, keeping original documents provided by the applicant will serve as a historical reference file. Components will notify OHA via the OHA credentialing mailbox at ohacredentialing@hq.dhs.gov or by telephone regarding a health care providers change in status. In addition, OHA will review with Components status of health care providers against those identified on the spreadsheet and/or database annually.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more information than is necessary is collected for the purpose of verifying an applicant's medical credentials prior to approval as a DHS health care provider.

Mitigation: In the process of implementing the DHS Instruction 248-01-001, Medical Quality Management, OHA outlined steps to the credentialing process and identified the relevant and necessary data elements required to verify an applicant's medical credentials and have been limited to the forms as seen in Appendix I. No collection of SSN is required.

Collection of credentialing information is relevant and appropriate to the medical credentialing process. OHA will collect data elements for two types of Health Care Providers, EMS and Physicians, Pharmacists, Nurse Practitioners, Physician Assistants and Registered Nurses. DHS Employees who are medical care providers will submit the credentialing form to include all relevant supporting documents. OHA will verify credentials information provided by the applicant. The verification process for EMS medical care providers is limited to NREMT and state licensing agencies (if applicable) to verify credentials where as "health care providers" (physicians, pharmacist, nurses, other) require a more in-depth verification based on the professions requirements (e.g., Physician verification may include, but not limited to, post graduate, residency, state license, national certification/registration, Federal DEA/State CSR and basic and advanced life support training).

Data quality and integrity will only be as good as what was provided by the applicant on the credentialing application form. If noted inconsistencies, OHA will contact the applicant for clarification and/or request that the applicant correct records with the professional agency and then resubmit credentials package for consideration. OHA will have limited assets working credentialing issues and will implement an audit of records at least annually and/or every two years at renewal of DHS health care provider status. Integration of the audit and quality reviews will ensure that both DHS Component and OHA records are consistent and correctly reflect those members authorized as valid DHS health care providers.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

In accordance with the DHS Directive 248-01, Medical Quality Management, it is a requirement for DHS medical care providers to be medically credentialed prior to being allowed to provide designated medical services. The collected credentials information will be utilized for verification of an individual's professional and medical background to ensure there is no known medical liability/malpractice, scope of practice or licensing concerns. Should derogatory information or questions arise over clinical privileges or revoked or denied license or certifications regarding an applicant, OHA would contact the Component Supervisor to address such matters. In accordance with DHS Instruction 248-01-001, Medical Quality

Management, item VI, Section O Credentialing Process, appropriate measures will be addressed regarding failure of a DHS employee to meet qualifications.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

All verification documents will be maintained by OHA either electronically or paper. OHA will have the capability to query the credentialing database for total numbers of care providers throughout DHS, breakdown by Component, profession specific and for tracking and trending credential effective dates and to identify those close to expiration. Tracking of expiration dates will serve as a reminder to OHA and the Components to stay ahead of the credentialing requirements to ensure no lapses in "valid" DHS credentials occur. Having an expired status as a DHS health care provider may impact the DHS mission and the medical care provider's ability to provide medical services for, or on behalf of DHS.

3.3 Are there other components with assigned roles and responsibilities within the system?

No intra-Departmental sharing of information will occur. DHS employees who are health care providers will submit an application for consideration as a DHS health care provider to OHA. OHA will conduct primary source verification based on the information provided by the applicant on the credentialing form. DHS employee information will be captured in a database that will only be accessed by designated OHA employees performing primary source verification. Only designated OHA staff will manage and have access to the credentialing database. Inquires on whether a DHS health care provider is a valid DHS health care provider will be directed to OHA either by telephone or through the designated OHA Credentials mailbox (ohacredentialing@hq.dhs.gov).

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a potential risk that the DHS health care provider database has incorrect information associated with it.

Mitigation: DHS Component Heads will be responsible for the internal credentialing process within their Component. A system of checks and balances will be established to ensure that DHS health care providers under their purview have the approved DHS health care provider credentials. Upon verification and approval by OHA, the DHS health care provider will be issued a provider number, which will be tracked at OHA and at the Component level. Components will notify OHA via the OHA credentialing mailbox at ohacredentialing@hq.dhs.gov or by telephone regarding a health care providers change in status. At least annually, OHA and DHS Components will review records on those members authorized as a valid DHS health care provider. Any discrepancies noted will be acted upon and corrected immediately.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The credentialing form explicitly addresses the intended purpose and routine uses of the provided credentialing information and the applicant signs acknowledging the Privacy Act Statement and that the information provided is correct and is subject to verification.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

An individual consents to uses of their information by signing the statement on the credentialing form which states, "I understand that all information on this application is correct to the best of my knowledge and is subject to verification." In addition, as noted in the Privacy Act Statement on the credentialing form, furnishing the information is voluntary; however, failure to furnish the information will prevent DHS from permitting the applicant to function as an authorized DHS medical care provider.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an applicant may be unaware as to how their information will be used.

Mitigation: Applicants are given many forms of notice regarding the purpose and use of their information. Specifically, as part of the application process, each applicant will review the Privacy Act Statement at the bottom of the credentialing form which addresses the authority, purpose, routine uses as per OPM/GOVT-1, General Personnel Records, and disclosure of how information will be utilized. In addition, the applicant signs the form attesting that they "understand that all information on this application is correct to the best of my knowledge and is subject to verification." Further, this PIA, and the OPM/GOVT-1 SORN provides notice. Accordingly, the risk that individuals are unaware about the collection and use of their information is minimal.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

OHA will retain and manage active files on DHS Employees serving as a valid DHS health care provider throughout the credentialing coverage. DHS health care providers will be required to renew their credentialing verification every two years (this aligns with NREMT and other licensing agencies on

renewal of professional licensure). Renewal will consist of the same requirements outlined for initial verification, health care providers will be required to submit a new credentialing form to include supervisor signature. As part of the renewal process applicants will be given one month past the expiration date to allow for any delay in processing time through the respective licensing agencies. It is highly encouraged that Components implement an internal process for monitoring and tracking individual medical care providers under their purview for required training and expiration dates of professional licenses, credentials and/or registrations as appropriate. OHA will also internally track and query the credentialing database for expiration status and follow up as needed with the respective Component regarding health care provider status. OHA will retain all historical files (either paper or electronic) on credentialed DHS medical care providers until such time as they are no longer eligible (e.g., retire, transfer or change in position) to be credentialed and serve as a valid DHS health care provider. Components will notify OHA via the OHA credentialing mailbox at ohacredentialing@hq.dhs.gov or by telephone regarding a health care providers change in status. In addition, OHA will review with Components status of health care providers against those identified on the spreadsheet and/or database annually. OHA will follow OPM/GOVT-1 guidance for retention and disposal, items a - c for handling of both electronic and paper credentialing files.

5.2 Privacy Impact Analysis: Related to Retention.

Privacy Risk: There is risk that credentialing information is out-of-date and no longer accurate (e.g., lapse in license, certification and incomplete training requirements making the employee no longer eligible for a credential and to provide care for, or on behalf of DHS) or that too much information is retained.

Mitigation: In accordance with DHS Instruction 248-01-001, Medical Quality Management (MQM), DHS Component Heads ensure that employees have the qualifications and other credentials (licenses, certifications and/or registrations, relevant training and experience) necessary to perform designated medical services before they are permitted to deliver health care services for, or on behalf of the DHS. It is highly encouraged that Components implement an internal process for monitoring and tracking individual medical care providers under their purview for required training and expiration dates of professional licenses, credentials and/or registrations as appropriate. OHA will also internally track and query the database for expiration status and follow up as appropriate with the respective Component. OHA will also create a "red flag" mechanism for which to track those individuals soon to expire (e.g., 3-4 month window). DHS medical care providers are required to resubmit credentialing information for re-verification and renewal every two years. DHS Component Heads and OHA will collectively work together to ensure that DHS medical care providers submit for re-verification early to avoid invalid status as a DHS health care provider or lapse in license renewal status.

Medical credentialing information will be retained on the DHS health care provider during the time they are actively providing medical care services for, or on behalf of the Department and pertinent to their current assigned duties. Components will notify OHA in writing that the provider is no longer required to hold a valid DHS health care provider credential. The medical credentialing database will reflect "inactivation." All historical files will be either destroyed or processed in accordance with

OPM/GOVT-1, General Personnel Records, Retention and Disposal. Annual audits will be conducted with designated Component heads to validate DHS health care providers against Component internal files to prevent possible invalid DHS credentials. OHA will retain only active medical credentialing files; all files will be in a secure location, and/or locked file cabinet with only designated access; the credentialing database will be password protected and limited access by those with a need to know status.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The OHA credentialing process may require that external entities such as professional institutions, licensing and certification agencies be contacted as part of the verification process. In some instances only web-based sites will be utilized to verify the applicants license number, certification and/or registration. The sharing of information with external entities will be limited to providing applicant name, dates and license, certification and/or registration numbers as part of the verification process (no list of names will be submitted, verification will be on an individual basis). The designated OHA staff working credentials will create a tracking log of all contacts, recording names, date and time.

For routine purposes there would be no requirement to disclose or share information on DHS health care providers outside of DHS channels. Should another agency contact OHA to inquire about whether a DHS health care provider is credentialed, OHA will only verify that the member has a valid DHS credential to provide medical care for, or on behalf of DHS. No other release of information would be made.

If a DHS medical care provider was to undergo possible de-credentialing for scope of care and/or standard of care issues, Components may take adverse or disciplinary action(s) as appropriate regarding the individual. There may be a requirement to share information to federal, state, local, and professional licensing boards in the event a DHS medical care provider falsified information, failed to practice to the scope and standard of care as it relates to their skill and professional standards. In alignment with DHS Directive 248-01, Medical Quality Management a peer review would be conducted to determine if the standard of care was met in relation to patient care and competency level.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Routine use ii of the OPM/GOVT-1 SORN allows DHS to disclose information to federal, state, local, and professional licensing boards, employment histories or concerning issuance, retention or revocation of licenses, certifications or registration necessary to practice an occupation, profession or specialty where an employee failed to conform to generally acceptable standards of professional medical practice as to raise reasonable concern for the health and safety of patients in the private sector or from another federal agency.

6.3 Does the project place limitations on re-dissemination.

As noted above, information provided above would be for individual cases where notification was made to a licensing agency or the NPDB for purposes related to the provision of care practices, adverse licensure actions, investigations, and other situations that are applicable to scope and standard of care practices. Any initial or ongoing actions against a DHS health care provider will be worked through the Components, ASHA/CMO and legal entities as appropriate.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Any release of information/files will be annotated and logged accordingly with who signed them out, to whom, date/time and reason.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: As per DHS Instruction, 248-01-001, Medical Quality Management, in accordance with applicable federal law, Components take adverse or disciplinary action(s) as appropriate, this might mean forwarding information to HIPDB/NPDB and professional licensing agency of actions. As noted in 1.2 and 6.2 under OPM/GOVT-1, General Personnel Records, Routine use (ii.) allows DHS to disclose information to federal, state, local, and professional licensing boards, employment histories or concerning issuance, retention or revocation of licenses, certifications or registration necessary to practice an occupation, profession or specialty where an employee failed to conform to generally acceptable standards of professional medical practice as to raise reasonable concern for the health and safety of patients in the private sector or from another federal agency.

Mitigation: As noted above there are instances under OPM/GOVT-1, General Personnel Records, Routine use (ii.) which allows DHS to disclose information. Any release of information/files will be annotated and logged accordingly with who initiated the action, person signing them out, date/time, to whom, and for what reason. The log will be maintained in the secure cabinet with medical credentialing files. In the event of a disciplinary and/or de-credentialing action, the respective Component will ensure that appropriate measures are taken notify the professional agencies. If a DHS health care provider is de-credentialed, appropriate actions would be taken to update the credentialing database to reflect deactivation of the health care provider. Log entries would be made to ensure appropriate chain of custody for the de-credentialed health care provider files.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

When a DHS Employee who is a health care provider submits their individual credentials package for consideration, the credentialing form will include a Privacy Act Statement informing the individual that the information collected will be utilized for medical credentialing purposes, to include verification of professional licenses, certifications and/or registrations and reasons for disclosure of information. The Component will retain the original copies of medical credentialing information submitted forward to OHA for consideration. At any time the member may request a copy of their individual credentials file through the authorized Component official to review for content and accuracy. The Component and/or individual DHS health care provider can also submit a formal request through the OHA Credentialing mailbox ohacredentialing@hq.dhs.gov for a copy of credentialing files retained by OHA. Additional avenues for obtaining and requesting personal information can be made formally through the Privacy Act/DHS Freedom of Information Act Officer (FOIA) at www.dhs.gov/foia.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As noted above in 7.1 the DHS health care provider has several options to review credentialing files for content and accuracy. Additionally, should the records reflect incorrect licensing information, the medical care provider will be required to resolve those inaccuracies with the respective professional licensing board and subsequently provide the corrected information to OHA to ensure that updates are made to the individual's files.

7.3 How does the project notify individuals about the procedures for correcting their information?

Should inaccuracies be noted during the OHA verification process, OHA will contact the DHS Employee to review their specific application information to determine where inconsistencies are noted. As noted in 7.2, if the inaccuracy involves professional licensing information, the individual will be responsible to work that process and provide OHA with the corrected or updated information. OHA will make all attempts to work with the individual DHS medical care provider to ensure the medical credentialing information is correct. Any requests to correct medical credentialing information can be made through OHA Credentialing mailbox at ohacredntialing@hq.dhs.gov.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: DHS employees who are health care providers will provide OHA with required information needed to conduct primary source verification prior to approval as a DHS health care

provider. Information obtained from the credentialing form will be transcribed into an OHA credentialing spreadsheet. There is risk that in the transcription process that incorrect information could be entered.

Mitigation: As noted in earlier responses for Section 7.0 Redress, initial credentialing information will be obtained from the medical care provider credentialing form. There is a possibility that information is incorrect from that work sheet, or upon transcription to the OHA credentialing spreadsheet. If upon verification of the DHS medical care provider information there are noted inconsistencies, OHA will contact the medical care provider to seek clarification of their information. If the inaccuracy is with the professional licensing board, OHA will request the individual take action to correct the problems and provide OHA with the updated information. OHA will work with the Component and individual DHS medical care providers to ensure that information is current and accurate. If the individual requests a copy of their credentials files a formal request can be submitted to the OHA Credentialing mailbox at ohacredentialing@hq.dhs.gov. Requests for credentialing files by the individual will be logged in and tracked for accountability purposes.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Designated OHA employees will have "full" access to the Component medical credentialing information; limited users will have "read-only" access. OHA credentialing staff will conduct quarterly audits on information files, review access logs and ensure that should there be a request for any DHS medical care provider information that documentation and all accounts of the transcription are appropriately logged for accountability purposes.

ASHA/CMO or other senior leader may request that the medical credentialing spreadsheet and/or database be queried for specific de-identified information related to the provision of care such as numbers of providers across DHS or Component specific, breakout by types of professionals, whether EMS, MD, PA, NP or RN and to the types of skill sets. No PII would be included in this data search and the information would be for DHS purposes only so as not to compromise any sensitive mission activities.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS personnel are required to participate in annual privacy and security awareness training. Users of the OHA medical credentialing database will have training as it relates to data entry and security compliance of the system and to ensure password protection measures are in place and adhered to.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only designated OHA employees responsible for all aspects of the medical credentialing program, to include spreadsheets and/or equivalent database and retained files will be the end-users.

Given DHS health care provider mission requirements to sometimes work across borders and state lines, there may be instances that local state EMS officials inquire about credentials. There is a possibility that state EMS officials may contact OHA to verify whether the DHS health care provider holds a valid DHS credential. The only sharing of information per this request would be for OHA to verify that the DHS health care provider has a valid DHS credential to provide care for, or on behalf of DHS.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Not applicable for this system.

Responsible Officials

Michelle D. Adams, Project Manager

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix I – DHS EMS and Health Care Provider Credentialing Forms