Privacy Impact Assessment
Emergency Response Service 2.0 (EMRS-2)

- Version: 1.4
- Date: December 2017
- Prepared for: USDA APHIS VS Emergency Response Management Service 2.0 (EMRS-2)

Technology, Planning, Architecture, & E-Government

Privacy Impact Assessment for the Emergency Management Response Service 2.0 (EMRS-2)

December 2016

Contact Point
Elinor Gallelli
APHIS Veterinary Services
United States Department of Agriculture
970-494-7333

Reviewing Official
Tonya G. Woods
APHIS Privacy Act Officer
United States Department of Agriculture
(301) 851-4076

Danna L. Mingo
Privacy Compliance Officer
Information Security Branch
United States Department of Agriculture
(301) 851-2487

Abstract

The Emergency Management Response Services 2.0 (EMRS-2) is a Major Application used by the APHIS Veterinary Services (VS) to manage and investigate animal disease outbreaks in the United States. The system is used by Federal, State, Tribal, and local animal health officials and human health officials. This Privacy Impact Assessment (PIA) is being completed following the Privacy Threshold Analysis (PTA) conclusion requiring a PIA for EMRS-2 to meet federal privacy compliance requirements.

Overview

The EMRS-2 is an incident management data collection system used by Veterinary Services to manage and investigate animal disease outbreaks and instances of foreign animal disease (FAD) in the United States. The EMRS-2 business requirement has three main process domains: Investigation management, Lab Submission management, and Resource management.

EMRS-2 is custom built within the Microsoft Dynamics CRM (MSCRM) platform, and is accessed by approved users via Microsoft Internet Explorer. EMRS-2 also utilizes the BING mapping Web service graphical user interface for easy visualization of work areas. Primary users of EMRS-2 are Federal and State veterinary medical officers, animal health technicians, and various disease specialists and epidemiologists from APHIS and from State cooperators. In an animal disease emergency, VS could potentially enlist the assistance of accredited private veterinary practitioners who assist with disease exclusion, detection, and control.

1 Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Information includes name; address (including city), county, state, postal code, latitude/longitude coordinates; premises identification number; and telephone number. The EMRS-2 may also contain the name and telephone number of the person(s) who provided the initial report concerning the premises, and the name, telephone number, and e-mail address of the person responsible for the investigation of the premises. EMRS-2 also contains information about APHIS employees who may be deployed as members of Incident Command System (ICS) teams and their position assignment.

1.2 What are the sources of the information in the system?

Owner or operator of the premises where the animal(s) subject to investigation are located and APHIS VS employees, referring contact, and case coordinator.

1.3 Why is the information being collected, used, disseminated, or maintained?

Data is used by the VS to manage and investigate animal disease outbreaks in the United States. The system is used by Federal, State, Tribal, and local animal health officials (and human health officials) for:

- Routine reporting of Foreign Animal Disease (FAD) investigations
- Surveillance and control programs
- State-specific disease outbreaks
- National animal health emergency responses

1.4 How is information collected?

State and local VS and Veterinary Officers and various disease program laboratories provide data for use in EMRS-2, depending upon the geographic extent of the particular animal disease outbreak, and dependent upon if an appropriate data sharing MOU is in place with USDA. The mapping module occasionally utilizes public data from the U.S. Geological Survey and other Federal resources available to the public.

1.5 How will the information be checked for accuracy?

Authorized federal, state, or temporary EMRS-2 personnel that collect and enter the data are responsible for the review and accuracy of the data. Information is obtained from either a customer or an employee and is often supplemented during an investigation by on-site visits, USPS database, or other address-validation databases. There are also limited data entry constraints to ensure entry completeness. APHIS employees also have access to the EMRS-2 Administrative module where they may edit and maintain their own employee profiles. EMRS-2 updates Employee Profiles via records in the Emergency Qualification System (EQS) and this is done quarterly (EQS gets their data from the National Finance Center (NFC) bi-weekly).

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

APHIS is an emergency response organization whose mission is to protect the health and value of U.S. agricultural, natural and other resources.

The Animal Health Protection Act (AHPA) (7 U.S.C.8301 et seq.) provides the authority for the Secretary to prevent, detect, control, and eradicate diseases, and pests of birds and other livestock to protect animal health, the health and welfare of people, economic interests of

livestock and related industries, the environment, and interstate and foreign commerce in birds, other livestock, and other articles.

Any additional authority comes from the specific state under which investigation is occurring.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy rights of the customer and employees will be protected by USDA, APHIS and VS management.

- Users accessing EMRS 2 must successfully authenticate using their e-Authentication PIV or e-Authentication username/password credential and be authorized with specific EMRS role(s).
- The application limits access to relevant information and prevents access to unauthorized information.
- Data is secured by means of encryption and access control. Access is controlled by:
- User ID and password or PIV card
- e-Authentication
- Access Control list
- Read and write authorization permissions that are specific to individual EMRS-2 electronic forms
- Location-specific servers
- Microsoft Dynamics CRM role based access control.
- The VS management team and National Preparedness and Incident Coordination Center management will determine when data needs to be consolidated and ensure

2 Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information

Data is used by VS to manage and investigate animal disease outbreaks in the United States. The system is used by Federal, State, Tribal, and local animal health officials (and human health officials) for:

- Routine reporting of Foreign Animal Disease (FAD) investigations
- Animal disease surveillance and control programs
- State-specific animal disease outbreaks
- National animal health emergency responses

When other Federal and State emergency response agencies assist USDA with an emergency disease outbreak, they may be allowed limited access to the data in EMRS-2. The access will depend upon the MOU in place and the need to know of the other agency. Data will be used for:

- Routine reporting of FAD investigations
- Surveillance and control programs

- State-specific disease outbreaks
- National animal health emergency responses

2.2 What types of tools are used to analyze data and what type of data may be produced?

Microsoft Dynamics CRM (MSCRM) includes customizations to allow users to visualize and understand data using GIS mapping to support situational awareness needs.

MSCRM also includes features to allow users to analyze data in various ways. The most basic analysis tool is the view. Users may customize views to display data sorted by specific field and display only the data in selected fields. Users may only view the data to which they have access based on their role, as defined in MSCRM. Users may also create charts and graphs to show trends and statistical information. Users can create dashboards to display information that is customized to their needs.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

EMRS uses Bing Maps for imagery only and utilizes no other Bing Map services.

2.4 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.

Data is secured by means of encryption and access control. Access is controlled by:

- User ID and password or PIV card
- e-Authentication
- Access Control list
- Read and write authorization permissions that are specific to individual EMRS-2 electronic forms
- Location-specific servers
- Microsoft Dynamics CRM role based access control.
- The VS management team and National Preparedness and Incident Coordination Center management will determine when data needs to be consolidated and ensure date is protected from unauthorized access.

3 Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Routine FAD data from EMRS-2 is expected to be retained on the server for an indefinite time. Employee data is maintained as long as employee is employed and may be maintained for up to

five years after employment ceases in case employee is re-employed during emergencies. After an animal outbreak, data is retained a minimal of twenty years for an active record, and ten years for inactive records.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

No. Records retention in this application has not specifically been approved by NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Risks associated with data retention are minimal and include the possibility of the data being accessed by unauthorized personnel. EMRS-2 uses role based access to mitigate this risk. The VS management team and National Preparedness and Incident Coordination Center staff, State Veterinarians and EMRS-2 team members and authorized users are all responsible for protecting the privacy rights of the customers and employees affected by the interface. The login interface reminds users of their responsibility every time they log in.

4 Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

EMRS-2 does not routinely share data with any USDA organization. However, in case of emergency disease outbreak internal agencies may be allowed limited access to the data in EMRS-2 as indicated in Section 5 of the PIA.

4.2 How is the information transmitted or disclosed?

The data will be retrieved through selection queries to:

- View Data
- Create reports
- Create maps of specific areas

Data can be retrieved only by personnel who successfully authenticate using their e-Authentication PIV or e-authentication username/password credential and are authorized with specific EMRS role(s). If data is retrieved via the email client no record of data queried is kept by individual must have user access and rights to access data. Data can be retrieved by a full text

search or a defined search. The full text search allows any data matching the entered data element to be retrieved. In the Investigation module, defined search data can be retried by: Premises ID, Reference Control Number, Premises, Name, Incident Group, or Incident Site. In the Administration module, defined search data can be retrieved by: employee, property, fleet vehicle, ledger, last name, first name, employee ID, nickname, title, organization, or section.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

In emergency disease outbreak situations where internal agencies assist EMRS-2 with management activities, there is a potential for information to be shared with unauthorized users. It is the intent of EMRS-2 that the uses of information remain in accordance with the stated purpose and use of the original collection at all times. Steps will be taken to ensure that access to the information system is provided only to authorized users. Data will be used by USDA, Federal and State FADDs, the laboratories, and animal health officials to document, manage, and communicate activities and findings while conducting routine foreign animal disease investigations.

5 Section 5.0 External Sharing and Disclosure

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

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

When other Federal and State emergency response agencies assist USDA with an emergency disease outbreak, they may be allowed limited access to the data in EMRS-2. The access will depend upon the MOU in place and the need to know of the other agency. As an example, during Incident Management Response efforts, data may be shared the Food and Drug Administration, the Department of Homeland Security, or an applicable state Department of Agriculture. Data will be used for:

- Routine reporting of FAD investigations
- Surveillance and control programs
- State-specific disease outbreaks
- National animal health emergency responses

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it

covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

APHIS-11 Emergency Management Response System

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The data will be retrieved through selection queries to:

- View data
- Create reports
- Create maps of specific areas

Data can be retrieved only by personnel who successfully authenticate using their e-Authentication PIV or e-authentication username/password credential and are authorized with specific EMRS role(s). If data is retrieved, no record of data queried is kept but individual must have user access and rights to access data. Data will be retrieved thru views, reports, and queries to view data, create reports and create maps. Users must be authenticated and have role based access to data which is limited to a need to know basis to the users business unit (generally state level access). Data can be retrieved through searching the fields that have been enabled to be indexed and searchable, and would not include any fields the users does not have access to based upon field level security.

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

The uses of information are in accordance with the stated purpose and use of the original collection. Data will be used by VS Federal and State FADDs, the laboratories, and animal health officials to document, manage, and communicate activities and findings while conducting routine foreign animal disease investigations.

6 Section 6.0 Notice

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

6.1 Was notice provided to the individual prior to collection of information?

Yes. The EMRS-2 notice is located at the ocio website under APHIS-11-Emergecny Management Response System

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

Yes. There is no penalty at the federal level if user refuses to provide information. Any consequences are enforced at the state level.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes. Information is collected only for specified circumstances or investigation, and this information is not utilized for any other purpose other than for those collected. Use of data is limited to the use for which it was collected and EMRS-2 staff does not release information unless there is an over-riding reason.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Banner and MOU with other Organizations

7 Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Any individual may obtain information from a record in the system that pertains to him or her. Request for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be

addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address above. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified of procedures at the point of data collection.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manger to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Once received by the VS the requests to correct information are treated as sensitive material in accordance with the formal redress methods. Any data used or furnished to others would need to be cleared through the Freedom of Information Act process

8 Section 8.0 Technical Access and Security

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

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

Access to EMRS-2 is based on Need-to-know and role-based access.

8.2 Will Department contractors have access to the system?

No

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

All USDA APHIS VS employees are required to complete Privacy and Security Training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The USDA APHIS VS EMRS-2 received Authority to Operate (ATO) on February 27, 2012 by completing an Assessment and Authorization. Renewal of the ATO for this system will be initiated before November 4, 2016.

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

In accordance with FIP 199/200 Moderate Baseline Security Controls. Some of the technical safeguards for EMRS 2.0 using Dynamics CRM is a security model that includes auditing, role-based views, field-level security, and division of security. This means any events, such as create, modified, soft deletion, users, old and new values are audited at the field level. Even the audit history on individual record and/or audit history summary is also tightly controlled with separate security settings to protect the integrity of the log. The security model only provides users with access only to the appropriate levels of information based on their role(s). Furthermore, views and field-level are role-based as well; preventing users from seeing, accessing, and/or making changes to individual fields or records they do not have access to. Finally, access control is a combination of eAuthentication (user credential and authentication) and authorization (EMRS-2 roles).

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The data will be retrieved through selection queries to:

- View data
- Create reports
- Create maps of specific areas

Data can be retrieved only by personnel who have logged in with their e-Authentication PIV or e-authentication username/password credential and have been authorized with specific EMRS role(s). If data is retrieved, no record of data queried is kept but individual must have user access and rights to access data. Data will be retrieved thru views, reports, and queries to view data, create reports and create maps. Users must be authenticated and have role based access to data which is limited to a need to know basis to the users business unit (generally state level access). Data can be retrieved through searching the fields that have been enabled to be indexed and searchable and would not include any fields the users do not have access to based upon field level security

9 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 and other technology.

9.1 What type of project is the program or system?

The project is a "web-enabled" application allowing USDA personnel, as well as external users with limited privileges, to access the application via the USDA eAuthentication system. Internal users login to the application using their PIV card and external users login with their eAuthentication account and password.

9.1 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Major Application – Animal Health/Incident Response Management.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementations.

This application does not employ technology which may raise privacy concerns.

10 Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" andM-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

EMRS uses Bing Maps for imagery only and utilizes no other Bing Map services

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

EMRS-2 does not receive any personally identifiable information from third part websites or applications.

10.10 Does the system use web measurement and customization technology?

EMRS-2 does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

EMRS-2 does not use web measurement and customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

EMRS-2 does not collect or transmit any PII data from any third party application.

Responsible Officials

Johnathan T. Zack
APHIS-VS
United States Department of Agriculture