Privacy Impact Assessment

National Animal Health Laboratory Network

Revision:1.0

APHIS

Date: January 18, 2008

USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: APHIS-VS-CEAH

System Name: National Animal Health Laboratory Network (NAHLN)

System Type: ☒ **Major Application**
☐ **General Support System**
☐ **Non-major Application**

System Categorization (per FIPS 199): ☐ **High**
☒ **Moderate**
☐ **Low**

Description of the System:

NAHLN Program Background

The National Animal Health Laboratory Network (NAHLN) forms part of a nationwide strategy to coordinate the work of all organizations providing animal health surveillance and testing services.

At the Federal level, the U.S. Department of Agriculture's (USDA) National Veterinary Services Laboratories (NVSL) serves as the national veterinary diagnostic reference and confirmatory laboratory. The State/university laboratories in the NAHLN perform routine diagnostic tests for endemic animal diseases as well as targeted surveillance and response testing for foreign animal diseases.

Networking these resources provides an extensive infrastructure of facilities, equipment, and personnel that are geographically accessible no matter where disease strikes. The laboratories have the capability and capacity to conduct nationwide surveillance testing for the early detection of an animal disease outbreak. They are able to test large numbers of samples rapidly during an outbreak and to demonstrate freedom from disease after eradication.

Key elements of the NAHLN system include increased and more flexible capacity for laboratory support of routine and emergency animal-disease diagnosis and official responses to bioterrorism events; standardized, rapid diagnostic techniques used at the State, regional, and national levels; secure systems for communication, issuance of alerts, and reporting; and modern equipment and experienced personnel.

Information technology systems support the NAHLN vision by providing electronic interconnectivity between diagnostic-sample collectors, NAHLN laboratories, and national databases. By utilizing data and messaging standards established by veterinary medical and public-health agencies, accurate and consistent diagnostic information is quickly and securely transmitted, aggregated, and available for decision makers and analysts.

Who owns this system? (Name, agency, contact information)

Dr. Elizabeth A. Lautner
National Veterinary Services Laboratory
(515)663-7301

Who is the security contact for this system? (Name, agency, contact information)

Terry Luckau
APHIS-VS-CEAH
(970)494-7330

Who completed this document? (Name, agency, contact information**)**
Kimberly Vander Haar
APHIS-VS-CEAH
(970)494-7347

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	**Yes**	**Yes**
Social Security Number	**No**	**No**
Telephone Number	**Yes**	**Yes**
Email address	**Yes**	**Yes**
Street address	**Yes**	**Yes**
Financial data	**No**	**No**
Health data	**No**	**No**
Biometric data	**No**	**No**
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	**No**	**No**
Are social security numbers embedded in any field?	**No**	**No**
Is any portion of a social security numbers used?	**No**	**No**
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	**No**	**No**

If all of the answers in Questions 1 and 2 are NO, STOP
You do not need to complete a Privacy Impact Assessment for this system and the answer to
OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets,
Part 7, Section E, Question 8c is:
3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

---

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Patient (animal) owner related data includes:
First Name, Middle Name, Last Name, Phone Number, Fax Number, Street Address, City, State, Zip Code, Country, E-Mail Address

Employee related data includes:
First Name, Middle Name, Last Name, Phone Number, Fax Number, Street Address, City, State, Zip Code, Country, E-Mail Address

Other data includes laboratory operations information, laboratory identification, laboratory location, test methods, test results, test instruments, patient (animal) information, patient emergency contact information, communication integrity information

4. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

$\boxtimes$ Yes
$\square$ No

5. Sources of the data in the system.
5.1. What data is being collected from the customer?

None

5.2. What USDA agencies are providing data for use in the system?

USDA-APHIS-VS-National Veterinary Services Laboratories

5.3. What state and local agencies are providing data for use in the system?

State veterinary diagnostic laboratories

5.4. From what other third party sources is data being collected?

None

6. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

$\boxtimes$ Yes

☐ No. If NO, go to question 7

6.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Accuracy verification: rules are enforced to confirm that the correct patient animal species and specimen types are tested for specific animal health programs, and that the correct test result type is reported for specific animal health programs.

Relevance verification: rules are enforced to confirm that the laboratory reporting test results is officially registered in the NAHLN laboratory registry.

Timeliness verification: information dissemination reports and graphs can be generated to track the average time between specimen collection date and date test result was reported.

Completeness verification: rules are enforced for required data elements to be submitted with each lab report.

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Accuracy verification: rules are enforced to confirm that the correct patient animal species and specimen types are tested for specific animal health programs, and that the correct test result type is reported for specific animal health programs.

Relevance verification: rules are enforced to confirm that the reporting laboratory is officially registered in the NAHLN laboratory registry.

Timeliness verification: information dissemination reports and graphs can be generated to track the average time between specimen collection date and date test result was reported.

Completeness verification: rules are enforced for required data elements to be submitted with each lab report.

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

The principal purpose of NAHLN is to support VS animal health program and surveillance activities for the purposes of detecting disease events and trends, controlling and/or eradicating endemic diseases, and determining prevalence of trade-significant diseases.

8. Will the data be used for any other purpose?

         ☐ Yes
         ☒ No. If NO, go to question 9

     8.1. What are the other purposes?

9. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President

         ☒ Yes
         ☐ No

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

         ☐ Yes
         ☒ No. If NO, go to question 11

     10.1.   Will the new data be placed in the individual's record (customer or employee)?

         ☐ Yes
         ☒ No

     10.2.   Can the system make determinations about customers or employees that would not be possible without the new data?

         ☐ Yes
         ☒ No

     10.3.   How will the new data be verified for relevance and accuracy?

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

The intended routine uses of NAHLN include supporting VS animal health program and surveillance activities for the purposes of detecting disease events and trends, controlling and/or eradicating endemic diseases, and determining prevalence of trade-significant diseases.

12. Will the data be used for any other uses (routine or otherwise)?

☐ Yes
☒ No. If NO, go to question 13

12.1.　　What are the other uses?

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

☒ Yes
☐ No. If NO, go to question 14

13.1.　　What controls are in place to protect the data and prevent unauthorized access?

The system has been categorized as a Moderate impact system and subject to 17 families of controls identified in the baseline security requirements of Annex 2 of NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

Among the controls employed are: role-based access controls, data encryption in transmission, physical and environmental protection, auditing, configuration management and contingency planning.

14. Are processes being consolidated?

☒ Yes
☐ No. If NO, go to question 15

14.1.　　What controls are in place to protect the data and prevent unauthorized access?

At this time, the system is in the operations /maintenance phase of its life cycle, minimum baseline security controls based on an approved security categorization will be implemented and the certified and accredited system.

DATA RETENTION

15. Is the data periodically purged from the system?

☐ Yes
☒ No. If NO, go to question 16

    15.1.   How long is the data retained whether it is on paper, electronically, in the system or in a backup?

    15.2.   What are the procedures for purging the data at the end of the retention period?

    15.3.   Where are these procedures documented?

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

The date the lab test was completed will be stored and evaluated to determine relevance and timeliness. Laboratories have the capacity to update laboratory findings, but only the organization that reported the information will have the right to update it. This will ensure accuracy and completeness over time.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

☒ Yes
☐ No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

☒ Yes
☐ No. If NO, go to question 19

    18.1.   How will the data be used by the other agency?

State laboratories will have the right to access the data, and only the data, they submitted to the system in order to review accuracy and completeness.

18.2.   Who is responsible for assuring the other agency properly uses of the data?

State laboratory system users are only provided the right to access their own data. It is assumed that each laboratory will properly use their own data.

19. Is the data transmitted to another agency or an independent site?

☐ Yes
☒ No. If NO, go to question 20

19.1.   Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

20. Is the system operated in more than one site?

☐ Yes
☒ No. If NO, go to question 21

20.1.   How will consistent use of the system and data be maintained in all sites?

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

Laboratory users will have access to data submitted by their, and only their, laboratory
VS Animal Health Program and Surveillance staff will have access to data appropriate for their region or program
Lab Data Transmission support staff will have access to the data
System and Database Administrators will have access to the data

22. How will user access to the data be determined?

User access will be controlled via role based, laboratory where employed, and regional responsibility access control. Criteria, controls and responsibilities have been

documented in user access matrices. Procedures have been defined in user guides associated with system modules.

> 22.1.　　Are criteria, procedures, controls, and responsibilities regarding user access documented?

> ☒ Yes
> ☐ No

23. How will user access to the data be restricted?

> The principle of least privilege is employed on this system. Each user's access will be restricted based on user role, laboratory where employed, and region of assigned responsibility for animal health. Only an Administrator would have access to all data. An extremely restricted number of administrators will be designated.

> 23.1.　　Are procedures in place to detect or deter browsing or unauthorized user access?

> ☒ Yes
> ☐ No

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

> ☒ Yes
> ☐ No

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e. office, person, departmental position, etc.)?

This responsibility lies with the system security organization consisting of the Agency Privacy Officer, Designated Approving Authority, Certifying Authority, Information System Security Program Manager and System Owner.

26. How can customers and employees contact the office or person responsible for protecting their privacy rights?

> Director, Freedom of Information and Privacy Act Staff
> Legislative and Public Affairs
> USDA: APHIS
> 4700 River Road
> Riverdale, MD 20737-1232

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

        ☒ Yes. If YES, go to question 28
        ☐ No

    27.1.   If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:
- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?

        ☐ Yes
        ☒ No. If NO, go to question 29

    28.1.   Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of customers?

       The system will allow for due process and comply with the American Disabilities Act (ADA) for Section 508 Compliance.

30. Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

        ☐ Yes
        ☒ No. If NO, go to question 31

    30.1.   Explain

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☒ Yes
☐ No. If NO, go to question 32

31.1.   How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

Data can be retrieved by employee number or name.

31.2.   Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

NAHLN anticipates that it will operate under its own system of records unless otherwise directed.

31.3.   If the system is being modified, will the SOR require amendment or revision?

If the system is modified in the future, the SOR Notice will be analyzed at that time to determine whether an amendment or revision is required.

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

☐ Yes
☒ No. If NO, the questionnaire is complete.

32.1.   How does the use of this technology affect customer privacy?

The system will not affect customer privacy.

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

<u>National Animal Health Laboratory Network</u>
(System Name)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____   10-21-08
System/Manager/Owner   Date
OR Project Representative
OR Program/Office Head.

_____   10/21/08
Agency's Chief FOIA officer   Date
OR Senior Official for Privacy
OR Designated privacy person

_____   10/21/08
Agency OCIO   Date