Privacy Threshold Analysis
and Privacy Impact Assessment

eCase SaaS

Version 1.1

January 18, 2014

Company Sensitive and Proprietary
For Authorized Use Only

Executive Summary

eCase SaaS is a Cloud Service Provider (CSP) offering that has undergone either a Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA). This document includes the PTA/PIA for eCase SaaS.

Document Revision History

Date	Description	Version	Author
01/18/2014	Initial Draft	1.0	RedPhone, LLC.
01/27	PIA Updated	1.1	AINS

Table of Contents

List of Tables

1. PRIVACY OVERVIEW AND POC

The following individual is identified as the eCase SaaS Privacy Officer and point of contact for privacy at AINS.

Table 2-1. eCase SaaS Privacy POC

Name	David Kruger
Title	Vice President
CSP / Organization	AINS
Address	806 W. Diamond Avenue Suite 400 Gaithersburg, MD. 20878
Phone Number	301.670.2300
Email Address	dkruger@ains.com

1.1. PRIVACY LAWS, REGULATIONS, AND GUIDANCE

A summary of laws, regulations related to privacy include:

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104-231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100-503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A-130, Management of Federal Information Resources, 1996
- OMB Memo M-10-23, Guidance for Agency Use of Third-Party Websites
- OMB Memo M-99-18, Privacy Policies on Federal Web Sites
- OMB Memo M-03-22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

Guidance on privacy issues can be found in the following publication:

- *NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

- FTC Fair Information Practice Principles
  http://www.ftc.gov/reports/privacy3/fairinfo.shtm

- Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)
  http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html

- Privacy and Security Law Issues in Off-shore Outsourcing Transactions
  http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf

1.2. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memo M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (date of birth and street address). A non-exhaustive list of examples of PII include:

- Social Security numbers
- Passport numbers
- Driver's license numbers
- Biometric information
- DNA information
- Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

2. PRIVACY THRESHOLD ANALYSIS

AINS performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the eCase SaaS components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by AINS can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

2.1. QUALIFYING QUESTIONS

1) Does the eCase SaaS collect, maintain, or share PII in any identifiable form?

☐ No
☒ Yes

2) Does the eCase SaaS collect, maintain, or share PII information from or about the public?

☐ No
☒ Yes

3) Has a Privacy Impact Assessment ever been performed for the eCase SaaS?

☐ No
☒ Yes

4) Is there a Privacy Act System of Records Notice (SORN) for this system?

☐ No
☒ Yes, the SORN identifier and name is: Correspondence Tracking System (CTS)

If answers to questions 1-4 are all "No" then a Privacy Impact Assessment may be omitted. If any of the answers to question 1-4 are "Yes" then complete a Privacy Impact Assessment.

2.2. DESIGNATION

☒ A Privacy Sensitive System

☐ Not a Privacy Sensitive System (in its current version)

3. PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment has been conducted for the eCase SaaS on January 18, 2014.

3.1. PII MAPPING OF COMPONENTS

eCase SaaS consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by eCase SaaS and the functions that collect it are recorded in Table 4-1.

Table 4-1. PII Mapped to Components

Components	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
eCase Application	Yes	Name, Address, phone number, email, etc	Case Management Tracking	FIPS 140-2 validated encryption module (AES)
FOIAXpress Application	Yes	Name, Address, phone number, email, etc	FOIA Data	FIPS 140-2 validated encryption module (AES)
PAL Application	Yes	Name, Address, phone number, email, etc	FOIA Data	FIPS 140-2 validated encryption module (AES)

3.2. PII IN USE

1) What PII (name, social security number, date of birth, address, etc.) is contained in the CSP service offering? Explain.

Types of information in the records include requesters' and their attorneys' or representatives' names, addresses, e-mail, telephone numbers, and FOIA case numbers; office telephone numbers, and office routing symbols of employees and contractors; names, telephone numbers, and addresses of the submitter of the information requested; unique case identifier; social security number (if provided by the requesting party).

- Requester details
  - Requester's name (First Name*, Middle Name, Last Name*)
  - Requester's organization
  - Requester's category* (e.g. Commercial Use, Educational Institution, News Media, Non-commercial Scientific Institution, Other
  - Requester's address (Street, City, State, Zip, Country*)

  - Requester's phone numbers (home, work, mobile, fax)
  - Requester's email
- Request details
  - Requester's name (First Name*, Last Name*)
  - Shipping address (Street, City, State, Zip, Country*)
  - Other address (Street, City, State, Zip, Country)-if different from shipping address
  - Billing address (Street, City, State, Zip, Country)-if different from shipping address
  - Request description (e.g. what the requester is asking for in their FOIA/PA request)
  - If fees/invoices and payment applies to a request, then the system may track the 'amount due', 'check#', 'bank name', credit card details('card type', 'card#', 'name on card', 'expiration month'

Additionally, eCase applications and FOIAXpress stores 'files' within the correspondence log for a request AND within the document management module (for responsive records), which may include but are not limited to the following:

- Correspondence from the requester (which may contain their name, address, phone#, etc.)
  - Incoming request letter
  - Clarification letter
  - Fee agreement letter
- Correspondence to the requester (which may contain their name, address, phone #, etc.)
  - Acknowledgement letter
  - Final response letter
  - Redacted responsive records
- Document management files
  - Original (un-redacted) responsive records
  - Redacted responsive records

2) Can individuals "opt-out" by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? Explain.

   System does not collect sensitive PII and it only collects basic personal information. These information is not shared by other agencies.

   ☐ Yes. Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

   ☐ No. Explain:

3.3. SOURCES OF PII AND PURPOSE

3) Does the CSP have knowledge of federal agencies that provide PII to the system? Explain.

   Yes, however, the system does not require these information for being functional but information like address, email address are entered into the system for it to assist the agencies and Department in tracking, managing and reporting correspondence, FOIA and Privacy Act (PA) requests.

4) Has any agency that is providing PII to the system provided a stated purpose for populating the system with PII? Explain.

   The system will assist the agencies and Department in tracking, managing and reporting FOIA and Privacy Act (PA) requests.

5) Does the CSP populate the system with PII? If yes, what is the purpose? Explain.

   No.

6) What other third party sources will be providing PII to the system? Explain the PII that will be provided and the purpose for it.

   N/A

3.4. ACCESS TO PII AND SHARING

7) What federal agencies have access to the PII, even if they are not the original provider? Who establishes the criteria for what PII can be shared? Explain.

   N/A (Information is not shared by external organization)

8) What CSP personnel will have access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP personnel to have access to the PII.

   No. CSP personnel will have direct access to any agency related information with the exception of those CSP personnel who directly works with that agency to support the system such as analysts, SME, technical lead with the authorization of agency representative.

9) How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain.

CSP personnel who directly works with that agency to support the system such as analysts, SME, technical lead with the authorization of agency representative. System provides an 'audit report', which details 'what event occurred' (e.g. the action taken), 'when' (e.g. date/time), where the event occurred (e.g. specific feature/function), the source of the event (e.g. user's IP address), and identify (e.g. user).

10) Do other systems share, transmit, or have access to the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing.

No

3.5. PII SAFEGUARDS AND LIABILITIES

11) What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? Explain.

The eCase system has multiple layers of security that protect content to the object level and can be applied to a user, group of users, or set as a general feature. Account access within the system is also limited in that users have a defined time period during which their access is actually active. This automatic feature will log out inactive users and disable their user account based on their access needs. The system can generate both usage and customized access reports that will report users who have been inactive or disabled from the system as needed.

Additionally, the audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records training requirements help prevent unauthorized access to data, browsing and misuse.

12) Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? Explain.

System Administrator. A training manual has been developed and distributed to users.

13) Does the CSP annual security training include privacy training? Does the CSP require contractors to take the training? Explain.

Users of the system receive annual Information Security Awareness training and Rules of

Behavior training. Some personnel may also receive computer security awareness training. No outside contractor involved.

14) Who is responsible for assuring safeguards for the PII? Explain.

System manager and Information system security officer, database system manager.

15) What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers be affected? Explain.

In most cases, there is minimal harm to the agency if privacy related data is disclosed, intentionally or unintentionally, because the PII is not sensitive (name, work phone number, email). In case of FOIA system, harm is minimal because the nature of the requests made would be FOIA related. For eCase applications, it can be harmful if agency decides to collect sensitive PII and if it requires by their respective business process, which mostly not the case and not required by system to function.

16) What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? Explain.

In most cases, there is minimal harm to the agency if privacy related data is disclosed, intentionally or unintentionally, because the PII is not sensitive (name, work phone number, email).

17) What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? Explain.

N/A

18) Is the PII owner advised about what federal agencies or other organizations share or have access to the data? Explain.

No other agencies have access to data.

3.6. CONTRACTS, AGREEMENTS, AND OWNERSHIP

19) NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not? Explain.

Customer contracts describe this principle referencing both agency privacy and data security guidelines and NITS SP 800-144 specifications.

20) Do contracts with customers establish who has ownership rights over data including PII? Explain.

Yes. Customer contracts clearly state that agency retains ownership rights over data and PII. Usually contracts have included the NIST guidelines.

21) Do contracts with customers require that customers notify the CSP if the customer intends to populate the service platform with PII? Why or why not?

To date, AINS knows in advance what type of data will be stored in our system prior to contract award.

22) Do CSP contracts with customers establish record retention responsibilities for both the customer and the CSP? Explain.

Yes, customer contracts stipulate the records retention requirements.

23) Is the degree to which the CSP will accept liability for expose of PII clearly defined in agreements with customers?

Our software license agreement spells out the limitations of liability. When required, AINS provides a certificate of insurance as part of our customer agreement.

3.7. ATTRIBUTES AND ACCURACY OF THE PII

24) Is the PII collected verified for accuracy? Why or why not? Explain.

Non-sensitive PII are collected and only format (such as email, phone) validation is done for accuracy.

25) Is the PII current? How is this determined? Explain.

The system stores metadata and associated files, which are obtained from agency officials; it is the responsibility of the originating office to ensure that the data entered into the system is current.

3.8. MAINTENANCE AND ADMINISTRATIVE CONTROLS

26) If the system is operated in more than one site, how is consistent use of the system and PII maintained in all sites? Are the same controls be used? Explain.

The system is being maintained at a single site at Gaithersburg data center. The primary

site will be replicated to a secondary site for backup purposes only or to provide coverage in the event of a significant outage of the primary system. All data transfer will be unidirectional from the primary server to the backup server. No additional data collection will occur on the backup server. As a result, the data in each location will be consistent.

27) What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

Records for each of eCase system applications and FOIA are maintained in accordance with the applicable records schedule for the agency. For HUD, the retention period is 10 years.

28) What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? Explain.

Records are disposed of in accordance with the applicable departmental records retention schedule and NARA guidelines. Paper records are disposed of by shredding and electronic media are degaussed.

29) Is the system using technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)? Explain.

No.

30) How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain. N/A

31) Is access to the PII being monitored, tracked, or recorded? Explain.

System has an audit log that can be used to run reports on individual users' access to and actions within the system.

32) If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? Explain.

No

3.9. BUSINESS PROCESSES AND TECHNOLOGY

33) Does the conduct of this PIA result in circumstances that requires changes to business processes? Explain.

No

34) Does the completion of this PIA potentially result in technology changes? Explain.

No

3.10. PRIVACY POLICY

35) Is there a CSP privacy policy and is it provided to all individuals whose PII you collect, maintain or store? Explain.

The system data is owned by agency and their privacy policy is followed.

36) Is the privacy policy publicly viewable? N/A If yes, provide the URL:

3.11. ASSESSOR AND SIGNATURES

This Privacy Impact Assessment has been conducted by AINS and has been reviewed by the AINS Chief Privacy Officer for accuracy.

G. P. Sinha

_____

Assessor Name (Please Print)

_____ _____

Assessor Signature Date

_____ _____

Chief Privacy Officer Signature Date

3.12. ACRONYMS

Acronym	Definition
CSP	Cloud Service Provider
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
POC	Point of Contact
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
SORN	System of Records Notice

3.11. ASSESSOR AND SIGNATURES

This Privacy Impact Assessment has been conducted by AINS and has been reviewed by the AINS Chief Privacy Officer for accuracy.

G. P. Sinha

Assessor Name (Please Print)

Assessor Signature

2/13/14
Date

Chief Privacy Officer Signature

2/13/14
Date