US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/09/2025

OPDIV:

NIH

Name:

Symantec Data Loss Protection

PIA Unique Identifier:

P-6548441-059401

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Symantec Data Loss Protection (DLP) utilizes the Symantec Endpoint Prevent and the Symantec Network Discover to automate the monitoring, detection, and prevention of improper distribution or transfer of sensitive data. This prevents the loss of information at the NIH Institutes, Centers, and Offices (ICOs) and automates the management of internal controls, improving the efficiency of the NIH's compliance processes.

The Symantec Endpoint Prevent portion of DLP consists of deployed agents that monitors workstations, endpoints to track and monitor sensitive data. and The Symantec Network enumerates Discover enumerates sensitive data in various repositories such as file shares, SharePoint, Cloud Storage and application/database servers to identify exposed sensitive data.

Describe the type of information the system will collect, maintain (store), or share.

PII is captured in DLP through scanning and monitoring. Focusing scanning on:

Social Security Number (SSN) patterns.
Credit Card Number patterns.
Medical Record Number (MRN) patterns.

DLP captures information surrounding each file and meta-data it flags as violating a defined policy. This data includes personally identifiable information (PII) identifying the File Owner, which could pertain to NIH personnel or a member of the public, Social Security Number, Name, Phone Number, Mailing Address, E-mail Address, MRNs, Employee Type (Contractor, Federal, Visitor etc.), IC Name, grant numbers, and Credit Card Number(s).

Additionally, the meta data includes access dates associated with the file (created, modified, and accessed), and the access rights associated with the file. DLP maintains a connection with The NIH Enterprise Directory (NED) and uses the connection to capture the PII of the File Owner defined in the meta-data of the violating file. NED maintains its own PIA.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collects unique user credentials and stores them in an encrypted format. The IAM Service is an essential service which facilitates and governs network access to various resources.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The Symantec Data Loss Protection (DLP) utilizes the Symantec Endpoint Prevent and the Symantec Network Discover to automate the monitoring, detection, and prevention of improper distribution or transfer of sensitive data. This prevents the loss of information at the NIH Institutes, Centers, and Offices (ICOs) and automates the management of internal controls, improving the efficiency of the NIH's compliance processes.

The Symantec Endpoint Prevent portion of DLP consists of deployed agents that monitors workstations, endpoints to track and monitor sensitive data. and The Symantec Network enumerates Discover enumerates sensitive data in various repositories such as file shares, SharePoint, Cloud Storage and application/database servers to identify exposed sensitive data.

PII is captured in DLP through scanning and monitoring. Focusing scanning on:

Social Security Number (SSN) patterns.
Credit Card Number patterns.
Medical Record Number (MRN) patterns.

DLP captures information surrounding each file and meta-data it flags as violating a defined policy. This data includes personally identifiable information (PII) identifying the File Owner, which could pertain to NIH personnel or a member of the public, Social Security Number, Name, Phone Number, Mailing Address, E-mail Address, MRNs, Employee Type (Contractor, Federal, Visitor etc.), ICO Name, grant numbers, and Credit Card Number(s).

Additionally, the meta data includes access dates associated with the file (created, modified, and accessed), and the access rights associated with the file. DLP maintains a connection with The NIH Enterprise Directory (NED) and uses the connection to capture the PII of the File Owner defined in the meta-data of the violating file. NED maintains its own PIA.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collects unique user credentials and stores them in an encrypted format. The IAM Service is an essential service which facilitates and governs network access to various resources.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Employee Type
ICO Name
Credit card number
Grant numbers

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose is to prevent unauthorized data ex-filtration. The DLP system detects unprotected (unencrypted) unauthorized transmissions and repositories of 3 major types of sensitive data: SSN, CCN, NIH Medical Record Numbers (MRN). As well as unapproved grant application numbers.

The remediation of the violating file through reporting to the file owner, and follow-ups with appropriate training.

Describe the secondary uses for which the PII will be used.

PII is used, secondarily, to create aggregated reports for monitoring trends and compliance.

Identify legal authorities governing information use and disclosure specific to the system and program.

42 U.S. Code § 241
42 U.S. Code § 281
42 U.S. Code § 282
42 U.S. Code § 284
OMB M-17-12

OMB M-21-31
E.O. 14028

Are records on the system retrieved by one or more PII data elements?

09-90-1701, HHS Insider Threat Program Records

OPM GOVT-1, General Personnel Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A. The data collected is not part of a solicitation.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The DLP is not a source system. Systems that are scanned provide processes to notify individuals that their PII will be collected. Additionally, individuals are notified when they enter into a business relationship with NIH.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no opt-out option. The DLP is not the source system. Individuals are notified when they enter into a business relationship with NIH.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The DLP is not a source system. Systems that are scanned provide processes to notify individuals when changes occur. Additionally, individuals are notified when they enter into a business relationship with NIH.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals can call the NIH Help desk or NIH Privacy Office at: privacy@mail.nih.gov

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The DLP is not a source system. Systems that are scanned provide processes for periodic reviews of PII.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

DLP follows NIH policy to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

DLP follows NIH policy to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Administrators receive vendor training and hold industry security certifications.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

07-213, Cybersecurity logging records. Cybersecurity event logs. Destroy when 30 months old. Longer retention is authorized for business use (DAA-GRS-2022-0005-0002).

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: Determinations and access are made based on role-based access controls and least privilege. Administrators grant user rights based on the minimum amount of PII necessary to perform their job. Users are also required to hold security certifications.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.)