NHS
Counter Fraud Authority

LogRhythm Security Incident Event Management

Data Protection Impact Assessment

May 2021

V4:0 Published Version

**NHS fraud.
Spot it. Report it.
Together we stop it.**

Executive Summary

This document contains information in relation to the LogRhythm Security Incident Event Management system. (LogRhythm SIEM)

The purpose of the LogRhythm system is to act as a SIEM (Security Incident Event Management) system. This means that it collects logs from multiple sources and keeps them together and can run them against different criteria such as rules and policies. This allows for the easy management and monitoring of a large environment by having all of the data in one place.

The processing involved in the LogRhythm system includes the collecting of logs from various sources. The method can vary from the usage of a collector to the Syslog inbuilt feature of some applications. This collection includes the likes of Event Logs, System Logs and Windows Logs. This can be from a variety of systems including servers, computers and firewalls. The SIEM then processes these logs using either pre-defined rules or user created ones. These rules can be used to trigger alerts or to display results to try and identify patterns or trends.

This kind of system will only contain system or event logs.

The DPIA was originally completed in 2018 and it remains current. Version changes have been as a result of redactions, and there have been no amendments to the use or functionality.

This document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (May 2018).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: **'OFFICIAL–SENSITIVE'**

The document is subject to CROWN COPYRIGHT. It is provided in confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

Table of contents

Document Control					
Completed By	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Security & Operational Support Analyst	LogRhythm Security Incident Event Management	DPO	V0.1	16/10/2018	All
Security & Operational Support Analyst	LogRhythm Security Incident Event Management	DPO	V0.2	08/11/2018	Review and update of all sections
Security & Operational Support Analyst	LogRhythm Security Incident Event Management	DPO	V1.0	28/11/2018	Final
Security & Operational Support Analyst	LogRhythm Security Incident Event Management	DPO	V2.0	31/03/2019	Amendments prior to publication
Security & Operational Support Analyst	LogRhythm Security Incident Event Management	DPO	V3.0	11/11/2019	Final review and redaction
Security & Operational Support Analyst	LogRhythm Security Incident Event Management	DPO	V4.0	01/05/2021	Further redaction for external publication

Prefix	
Reference:	DPIA / Log Rhythm Security Incident Event Management
Date:	May 2021
Author:	Security & Operational Support Analyst
Data Owner:	Information System and Analytics Manager
Version:	4.0
Supersedes	3.0

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	May 2018	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.

2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also effect other fundamental rights and interests:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy**, **unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[1]…"

5. Under GDPR you must carry out a DPIA where for example you plan to:

- process special category or criminal offence data on a large scale.

6. The ICO also requires a DPIA to be undertaken for example, where you plan to:

- use new technologies;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

[1] GDPR - Recital 75

8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

9. This DPIA is related to the NHSCFA RMADS, which outline the threats, risks and security countermeasures in detail. The RMADS was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

LogRhythm General Description

10. The purpose of the LogRhythm system is to act as a SIEM (Security Incident Event Management) system. This means that it collects logs from multiple sources and keeps them together and can run them against different criteria such as rules and policies. This allows for the easy management and monitoring of a large environment by having all of the data in one place.

11. The processing involved in the LogRhythm system includes the collecting of logs from various sources. The method can vary from the usage of a collector to the Syslog inbuilt feature of some applications. These collections includes the likes of Event Logs, System Logs and Windows Logs. This can be from a variety of systems including servers, computers and firewalls. The SIEM then processes these logs using either pre-defined rules or user created ones. These rules can be used to trigger alerts or to display results to try and identify patterns or trends.

12. This kind of system will only contain system or event logs.

13. For security and confidentiality purposes, the database is only accessed by approximately 10 members of staff from NHSCFA, which includes the database administrators.

14. This is the only DPIA to be completed on the LogRhythm and it has been carried out by the Information and Records Management Officer, in consultation with Security and Operational Support Analyst and the Information Governance and Risk Management Lead.

15. The LogRhythm, in addition to GDPR is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

16. To ensure the LogRhythm meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

[2] Version 0.3 (20180209)

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The LogRhythm system aims to provide a single point where logs from various systems can be gathered in one place making them both easier to monitor and manage. This also allows for specific rules and policies to be applied to each of these logs which allows for the filtering of results down to only relevant data. This system can also be used for triggering alerts on unusual/known bad events. For example, a range of IPs could be set as known bad IPs and an alert would be triggered if any logs involving these IPs were received. This involves the processing of system logs from various computers, be they servers, firewalls or user systems.

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?

2. What is the source of the data?

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

4. Why types of processing identified as ‘likely high risk’ are involved?

The Logs are collected either through the usage of Log Collectors or through other methods such as Syslog. This is done with very limited impact on system performance.

The sources of the data are the systems themselves. Specifically the event logs on the systems such as System Logs, Application Logs and Security Logs.

The data will be kept internally.

It is not high risk.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

The data will involve IP addresses, usernames, port numbers and actions being taken. No criminal or sensitive data is being processed or stored within this application. File names might be stored but the contents of said files are not.

It will collect all logs from any system. These logs will then be sorted into categories and risk ratings which can be used to identify important logs.

All the time.

The logs are kept active for 3 months. Then they are archived and stored for an unspecified period of time.

All users will generate logs when performing activity.

All business locations.

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?

2. How much control will they have?

3. Would they expect you to use their data in this way

4. Do they include children or other vulnerable groups?

5. Are there any prior concerns over this type of processing or security flaws?

6. Is it novel in any way?

7. What is the current state to technology in this area?

8. Are they any current issues of public concern that you should factor in?

9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

The individuals impacted are colleagues and external users of IT systems..

They control what logs are produced by their actions, a log is only produced when an action is taken that would produce one.

Yes, it is mentioned on the Acceptable Use Policy with which they agree to comply when signing in.

No vulnerable groups data is collected.

There are no concerns over this type of processing. It is a standard kind of processing which is accepted as being required for overseeing a large estate of computer systems.

SIEM Solutions are a recognised and accepted part of the IT Industry. They are used to collect and monitor logs from across the estate. This is seen as a necessity for threat and trend analysis for use in detecting and monitoring attacks against and compromises of the network.

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

3. What are the benefits of the processing, for you and more broadly?

We intend to monitor the estate for any unusual or dangerous activity on our systems. Some rules in place detect known malware related IP addresses whereas others are used to detect anomalous activity which could indicate unknown malware. It is also used to detect issues with systems and to help narrow down where these issues began.

The individual will likely not see the effects of the system as it is mainly intended to keep the network itself safe. Users may notice activity from this when system issues are identified and rectified.

The benefits of this type of processing are that it allows us to effectively manage our IT estate. It allows for the collection of logs from multiple systems and for us to gather them in one place where we can identify issues and anomalies. This kind of processing makes it easier and faster to identify issues on the estate and to quickly remedy them, potentially before they become significant.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

2. Who else do you need to involve within your organisation?

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

LogRhythm is providing a service that is required as part of the security policy of the organisation which has been agreed upon previously. Due to this the implementation of this software to provide the service did not require the approval of stakeholders.

Only the security and systems team require involvement for the implementation of this software.

The processors are part of the security and systems teams.

We do not plan on consulting security experts. We consulted the supplier regarding the setup of the software and had their assistance in the initial setup and use their documentation to assist with further configuring the software.

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

2. Does the processing actually achieve your purpose?

3. Is there another way to achieve the same outcome?

4. How will you prevent function creep?

5. How will you ensure data quality and data minimisation?

6. What information will you give individuals?

7. How will you help to support their rights?

8. What measures do you take to ensure processors comply?

9. How do you safeguard any international transfers?

The defined lawful basis for the processing as identified in Article 6(1) of GDPR would be:
Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

This is part of our internal security policy and is required to ensure the safety and security of our network.

It does achieve its purpose. Through the use of rules and policies we are able to monitor any suspicious or important activity. One example being that we get alerts through whenever logs are processed that involve suspicious IP Addresses.

The other way to achieve this would be to manually check all logs which is not a viable idea. The other alternative would be to use similar software to achieve this result such as SPLUNK however the processing would be largely the same, just with a different supplier.

A limited number of users will have access to the application to perform specific tasks. Due to this the chances of function creep are low.

Data quality is ensured by the logging system done before the information is received. If any issues are noticed they can be identified and resolved. Data is only collected from relevant log sources.

Individuals have access to the Acceptable Use Policy which covers this kind of data processing.

The data is not personal.

No international transfers are conducted.

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
External Internet Based Attacker – Gaining access to LogRhythm. This can allow an attacker to view log data and potentially build a network diagram of our infrastructure through information they gain from this. They would not be able to compromise any personal or confidential information.	Possible	Significant	Medium
LogRhythm User (Admin) – Through accident or intent a privileged user uses the service in a way that can cause damage to the processes or the organisation. This damage is limited to configuring rules and disabling or adding log sources. Logs themselves cannot be deleted. Log Sources cannot be deleted, only disabled.	Remote	Severe	Medium
Physical Intruder – In the event of a physical intruder the system could suffer from a denial of service due to damage or theft. Older data is archived to other systems and as such would not be lost. Newer data (within the recent three months) would be lost. Although very recent data would be stored on the log sources and could be recovered. The data loss would not contain personal or confidential data and would only aid in the construction of a network diagram for potentially further attacks.	Remote	Severe	Medium
Environmental Disaster – Due to an unforeseen disaster, be it intentional (Arson) or a natural disaster (Flood), the server could be damaged or destroyed. This would results in a denial of service for this system and data loss. As with above, data loss would primarily be limited to the newest data, some of which could be recovered.	Remote	Severe	Medium

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	**Effect on risk** Eliminated, Reduced, Accepted	**Residual risk** Low, Medium, High	**Measure approved** Yes/No
Continual assessment of opportunities to improve network security.	Reduced	Medium	
Continual monitoring of access rights given to staff and removal of access where it is no longer required.	Reduced	Medium	

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:	Trevor Duplessis 28 November 2018	If overruled, you must explain your reasons
Comments: I am satisfied having reviewed the DPIA that a comprehensive assessment has been undertaken of the system. Access to the software system is restricted to the IT Administrators and the Information Security Team, which means individual account usage, can be fully audited and access removed when no longer required. The information collected will not be personal information. While older system data is archived the system will still be kept under review for monitoring purposes.		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the LogRhythm roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Information System and Analytics Manager
Senior Responsible Officer (SRO) Information Risk Owner (IRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Information Security Lead
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. The purpose of the LogRhythm system is to act as a SIEM (Security Incident Event Management) system. This means that it collects logs from multiple sources and keeps them together and can run them against different criteria such as rules and policies. This allows for the easy management and monitoring of a large environment by having all of the data in one place.

2. This system contains data and event logs which contain IP Addresses, ports, usernames and types of events.

3. The impact level of the Log Rhythm System was assessed as CONFIDENTIAL and it can only be accessed internally.

4. The following measures briefly describe what controls have been implemented to protect the LogRhythm System and the personal data recorded:

    a. All off site back-ups are secure as they can only be opened via the encryption key.

    b. The System is only accessed by approximately 10 members of staff from NHSCFA, which includes the database administrators

    c. The LogRhythm System does have any direct interconnections with other NHSCFA systems and applications

    d. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.

5. It is assessed that there are no residual privacy risks to the personal data used by the LogRhythm System.

6. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

7. The purpose of the LogRhythm system is to act as a SIEM (Security Incident Event Management) system. This means that it collects logs from multiple sources and keeps them together and can run them against different criteria such as rules and policies. This allows for the easy management and monitoring of a large environment by having all of the data in one place.

8. The Information Security team has responsibility of the LogRhythm system.

9. Information in the Database/System could include;

- IP Addresses
- Ports
- Event Types
- Usernames
- Hostname

This list is not exhaustive

10. Also list any sensitive data:

N/A

11. The measures that have been implemented to protect the Personal Data are:

a. Access is restricted to approximately 10_members of staff within NHSCFA including the database administrators

b. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

12. The LogRhythm System is subject to NHSCFA Data Handling and Storage Policy.

13. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

14. Access is restricted to approximately 10 members of staff within NHSCFA including the database administrators.

Section 5: External Sharing and Disclosure of Data

15. The only information shared with external organisations, would be with the *police* if it was requested for the administration of justice.

Section 6: Notice/Signage

16. NHSCFA's Acceptable Use policy provides notice that this kind of data collection is conducted.

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this System and therefore outside the scope of this DPIA.

Section 7: Rights of Individuals to Access, Redress and Correct Data

18. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

19. It is unlikely that many access requests will be received as there is no personal data recorded.

20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

21. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

22. The security and technical access architecture of the Database/System is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official-Sensitive** and the hosting infrastructure is subject to CESG approved IT Security Health Check.

23. Access is restricted to internal staff only.

24. The technical controls to protect the database include:

a. Anti-virus protection;

b. Permission based access controls to shared drive.

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

25. The System does not hold personal and is located in the NHS Counter Fraud Authority data centre.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the Log Rhythm System, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

   a. The GDPR and the Data Protection Act in general;

   b. The Data Protection Principles;

   c. The interpretations of the Principles.

2. **This is not a recommendation but a requirement of law.**

3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.

4. The System processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, see Annex C

The Privacy and Electronic Communications Regulations

5. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

6. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

7. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

8. There are no residual privacy risks to the personal data recorded in the System. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA Information Systems and Analytics
Project	LogRhythm Security Incident Event Management (LogRhythm SIEM)

2. Contact position and/or name, telephone number and e-mail address.
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHSCFA
Phone Number	020 7895 4642
E-Mail	Trevor.Duplessis@nhscfa.gov.uk

3. Description of the system (initiative) being assessed.
(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

No personal data is collected by the LogRhythm SIEM solution. The only potentially identifiable information is the username of the user and the asset tag of the computer in use. This system is required to provide a service that meets our security objectives.

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHSCFA leads on a wide range of work to protect NHS staff from economic crime.

The purpose of the LogRhythm system is to act as a SIEM (Security Incident Event Management) system. This means that it collects logs from multiple sources and keeps them together and can run them against different criteria such as rules and policies. This allows for the easy management and monitoring of a large environment by having all of the data in one place.

Access is restricted to 10 members of staff within NHSCFA, including the database administrators.

5. What are the potential privacy impacts of this proposal?

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the LogRhythm System has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is the first DPIA carried out on the system.

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

*IMPORTANT NOTE:
'Personal data' means data which relate to a living individual who can be identified:
(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH