CAS Alerts Policy

Version	v1.2
Supersedes:	v1.1
Date Ratified by Board:	23rd November 2017
Reference Number:	PC24POL110
Title & Department of originator:	CAS Alerts Policy, Department of Quality & Patient Safety
Title of responsible committee/department:	Quality and Workforce Committee
Effective Date:	January 2018
Next Review date:	December 2022 or sooner or when there is a change in Policy or National Guidance
Target audience:	Both Clinical and Non-Clinical Staff
Impact Assessment Date:	31.08.2017
Summary	The policy details the arrangement for the receipt assessment, dissemination and completion of all alerts received from the Central Alerting System.

Version	Date	Control Reason	Title of Accountable Person for this Version
v1.0	September 2017	New Policy	Associate Director of Nursing
v1.1	June 2019	Reviewed policy and updated Company name	Associate Director of Nursing
v1.2	December 2019	Updated Policy to reflect changes in NHS department at a national level	Associate Director of Nursing

Reference Documents	Electronic Locations (Controlled Copy)	Location for Hard Copies
	Primary Care 24 Intranet / SOPs Clinical / Operations … **Delete as appropriate***	**Policy File, Wavertree Headquarters**

Consultation: Committees / Groups / Individual	Date
Leadership Team, Senior Management Team, Policy Group, Quality & Workforce Committee and the Board	23/11/2017

Contents Page

1 Introduction

1.1 The Central Alerting System (CAS) is an electronic, web-based system used by the National Health Service (NHS) for the issuing and cascading of various types of alerts, important public health messages and other safety critical information and guidance to NHS and other Health and Social Care providers.

1.2 The CAS system facilitates distribution of safety, emergency, medical device, drug and estates alerts, field safety notices, Chief Medical Officer messages and Dear Doctor letters issued by;

- The Medicines and Healthcare products Regulatory Agency (MHRA) – Drug Alerts
- NHS England
- Department of Health (DoH)
- NHS Department of Estates and Facilities (EFA)
- Patient Safety Alerts (PSA)
- Medical Device Alerts (MDA)

The CAS system issues patient safety alerts via the central alerting system to ensure that emerging patient safety risks are quickly communicated to organisations. It also acts as an educational and implementation resource and encourages information sharing between organisations. The potential areas addressed by these alerts include but are not limited to:

- Alerts for new or under recognised patient safety issues – where there is the potential to cause death or severe harm but which healthcare providers may not have knowledge or experience of the risk
- Alerts for widespread, common and challenging patient safety issues, not solved by alerts in isolation
- Alerts aimed at improving systems for clinical governance, reporting and learning – these alerts would aim to address significant risk in patient safety management systems

Dissemination of all external alerts, supplementary information, responses and actions are managed within the Governance Team. The alerts will be cascaded across the organisation using the internal email system.

1.3 Primary Care 24 (PC24) has a duty under the Health and Safety at Work Act 1974 to ensure the safety of its staff and anyone affected by the activities of the organisation; and this applies to the dissemination of information about hazards and issues contained within alerts.

1.4 Therefore, we are required to have a robust and effective system for the receipt, acknowledgement, assessment and, where relevant, the dissemination and completion of the alerts issued via the central alerting system.

1.5 It is the aim of PC24 to ensure that all alerts are communicated promptly to all relevant members of staff employed within the organisation and that action to comply with alerts is taken within the Department of Health (DoH) timescales in order to safeguard patients, visitors and staff from harm

1.6 PC24 recognises and accepts its duty to distribute and action safety alert notices received via the central alerting system. The organisation will apply the procedure outlined in the document to distribute and action alerts received from external agencies via the central alerting system.

1.7 This policy sets out the arrangements PC24 has in place for the management of all of the central alerts that it receives and/or disseminates.

2. Scope

2.1 Primary Care 24 (PC24) is committed to the delivery of a sustainable and assured process for swift implementation of alerts received via the central alerting system.

The process will include the completion of actions in accordance with time limits set by individual alerts and a monitoring and reporting process that would withstand internal / external interrogation.

3. Aim

3.1 The aim of this policy is to detail the arrangements for the receipt, assessment, dissemination and completion of all alerts received via the central alerting system.

3.2 The objectives are to ensure that PC24 has clear and defined arrangements for:

- The receipt, assessment, communication, dissemination and management of central alerts and the actions taken to comply with the alert are within the designated timeframes.
- Obtaining responses from Directors / Heads of Service / Practice Managers or nominated deputies following the dissemination of central alerts and other alerts
- Monitoring the completion of actions stated in the alert to ensure the safety of all those who deliver and receive services from PC24

4. Definitions

4.1 Alerts received via the central alerting system include the following:

4.2 **Central Alerts System (CAS)** is the electronic system developed by the DoH for sending important safety and device alerts to NHS and other Health and Social Care providers.

4.3 **Safety Alert Bulletins** is a generic term for alerts issued relating to medical devices, NHS Estates and NHS England alerts

4.4 **Medicines and Healthcare products Regulatory Authority (MHRA).** They are a DoH body, who regulates medicines and medical devices. They are recognised globally as an authority in its field; the agency plays a leading role in protecting and improving public health and supports innovation through scientific research and development

4.5 **DoH Estates and Facilities alerts (EFA)** are issued by NHS estates. They are a means of communication for safety information relating to engineering, installed services and building fabric

4.6 **CAS Alerts** are issued by NHS England on various patient safety and governance issues. There are three levels of alerts as identified below;

4.7 The CAS system has a three stage alert system:

Stage One Alert: Warning – This stage will 'warn' organisations of emerging risk. It can be issued very quickly once a new risk has been identified (by NHS England) to allow rapid dissemination of information. Typical actions required of organisations in a stage one alert would include:

- Consider if this (the risk issue) could happen / has happened locally
- Consider if action can be taken locally to reduce the risk
- Disseminate the warning to relevant staff, departments and organisations

Recipients will also be asked to share information with NHS England that may help to inform the development of stage two and three alerts, and potentially for wider dissemination to other providers. This might include:

- Share of learning from any root cause analysis (RCA)

- Sharing of local good practice that may act as a useful example to other providers

Stage Two alert: **Resource** –This may be issued some weeks or months after a stage one alert to help address the risks within this alert and could consist of:

- The sharing of relevant local information identified by providers from a stage one alert
- The sharing of examples of local good practice that mitigates the risk identified in the stage one alert
- Access to tools and resources that help providers implement solutions to the stage one alert
- Access to learning resources that are relevant to all healthcare workers and can be used as evidence of continuous professional development.

Stage Three alert: Directive – At this stage organisations will be required to confirm they have implemented specific actions or solutions to mitigate the risk. For those organisations that have already demonstrated good practice and locally developed appropriate risk mitigating strategies at stages one, or two, sign-off should be a formality. The actions will be tailored to the specific patient safety issue.

5. Roles and Responsibilities

5.1 The Board

5.1.1 The Board will ensure the following:

- That there are suitable and sufficient arrangements in place for the receipt, assessment, dissemination and completion of central alerts and other alerts received by the organisation
- There is a designated person to fulfil the role of Central Alerts Liaison Officer. The nominated Central Alerts Liaison Officer is the Clinical Audit & Effectiveness Lead and the deputy is the Quality Governance Facilitator

5.1.2 The Quality & Workforce Committee will monitor compliance with the policy

5.2 Chief Executive

5.2.1 The Chief Executive has overall responsibility for the effective implementation of this policy within the organisation and for having suitable and sufficient systems in place for the management of central alerts and other type of alerts received and disseminated by PC24.

5.3 Executive Director of Nursing and Quality

5.3.1 The Executive Director of Nursing and Quality has specific responsibility for:

- Ensuring that there are effective arrangements in place for the receipt, assessment and, where relevant, the communication, dissemination and completion of alerts
- Addressing and completing alerts within the designated timeframes

5.4 Medical Director

5.4.1 The Medical Director or nominated deputy has responsibility for:

- Receiving and assessing alerts received via the central alerting system in relation to alerts from the Chief Medical Officer, alerts from Dear Doctor Letters and alerts from the MHRA (Drug Alerts) and CAS alerts
- Ensuring that there are arrangements in place for the effective assessment and management of relevant medical device alerts
- Identifying which of the medical device alerts are applicable to PC24 and informing the Central Alerts Liaison Officer
- Ensuring that, when requested, evidence in relation to the actions taken to address alerts can be provided
- Advising the Central Alerts Liaison Officer which services should receive these relevant alerts
- Where applicable, auctioning and completing alerts and advising the Central Alerts Liaison Officer of the completion of these alerts within the designated timeframes stated on the alerts
- Ensuring that all of the required actions stipulated within the relevant alert are implemented within the designated timeframes so as to ensure compliance with the alert

- Informing the Central Alerts Liaison Officer that all of the required actions of a medical device alert / MHRA and CAS alerts are completed within the designated timeframes

5.5 Director of Business & Finance

5.5.1 The Director of Finance or nominated deputy has responsibility for:

- Ensuring that there are arrangements in place for the effective assessment and management of estates and facilities alerts
- Identifying which estates and facilities alerts are applicable to PC24 and informing the Central Alerts Liaison Officer of this within the designated timeframes
- Ensuring that all of the required actions stipulated within the relevant alert are implemented within the designated timeframes so as to ensure compliance with the alert
- Informing the Central Alerts Liaison Officer that all of the required actions of estates and facilities alerts are completed within the designated timeframes
- Ensuring that, when requested, evidence in relation to the actions taken to address alerts can be provided

5.6 Managers / Heads of Service / Practice Managers or nominated deputies

5.6.1. Managers and Heads of Service / Practice Managers or nominated deputies have responsibility for:

- Implementing this policy at a local level
- Ensuring that all relevant actions stipulated in an alert are communicated to their staff using appropriate methods of communication
- Ensuring that all actions are complied with and completed within the designated timeframes stated on the alert
- Informing the Central Alerts Liaison Officer that all actions stipulated in the alert have been completed within the designated timeframes
- Providing, upon request, evidence of the actions taken to comply with alerts

5.7 All staff

5.7.1 Where appropriate, all staff have a responsibility to abide by any actions taken in response to an alert that is relevant to PC24

5.7.2 Where necessary, they may also have to take appropriate actions within the required timeframes stipulated in an alert and submit a response to their Directors, Managers / Heads of Service / Practice Managers or nominated deputies

5.8 The Central Alerts Liaison Officer and/or their deputy

5.8.1 The Central Alerts Liaison Officer and/or their deputy has responsibility for:

- Acknowledging receipt of central alerts received via the central alerting system within the designated timeframes (two working days from the issue date)
- Receiving, assessing, communicating and disseminating central safety alerts (including alerts from the Chief Medical Officer and alerts from Dear Doctor Letters) and alerts issued via the CAS system to relevant Directors, Managers / Heads of Service / Practice Managers or nominated deputies
- Ensuring that, all Leads who have actions for the completion of central safety alerts and CAS directives are sent reminders
- Monitoring the completion of all actions on relevant central safety alerts and CAS directives
- Ensuring that the status of all relevant alerts are updated on the PC24 Governance CAS tracker system within the designated timeframes
- Update the PC24 Governance CAS tracker system that all stipulated actions within a relevant alert have been completed within the designated timeframes
- Ensuring that, when requested, evidence in relation to the actions taken to address alerts and CAS directives can be provided
- Maintaining a record of all of the alerts and CAS directives received by PC24 via the central alerting system and the management of them
- Ensuring that an up-to-date distribution list for central safety alerts and CAS directives is maintained
- Providing a bi-annual report to the Quality & Workforce Committee on the relevant central safety alerts and CAS directives received by PC24 and the actions taken
- If the alert is relevant and applicable to PC24, it will be sent to appropriate operational leads for information and/or action. It is clearly stated on the alert whether or not a response is required. A list of the personnel who should receive the alert is also listed on each alert

- Once the Central Alerts Liaison Officer has collated all responses to the alert and has reasonable assurance that all necessary actions, as stipulated in the alert, have been taken they will formally close the alert on the PC24 Governance CAS tracker system.
- Notifying the central alerting system of any changes of organisational changes to Central Alerts Liaison Officer personnel

6 Equalities and Health Inequalities Statement

PC24 is committed to an environment that promotes equality and embraces diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy has been implemented with due regard to this commitment. To ensure that the implementation of this policy does not have an adverse impact in response to the requirements of the Equality Act 2010 this policy has been screened for relevance during the policy development process and a full equality impact analysis conducted where necessary. PC24 will take remedial action when necessary to address any unexpected or unwarranted disparities and monitor practice to ensure that this policy is fairly implemented.

7 Personal Information Statement

PC24 is committed to an environment that protects personal information aspects in the development of any policy. When proposing change there is a new requirement for policy writers to investigate when the personal information aspect of the policy complies with the data protection principles in Schedule 1 of the Data Protection Act 2018. All individuals with responsibility for reviewing/writing policies should consider Privacy Impact Assessment compliance.

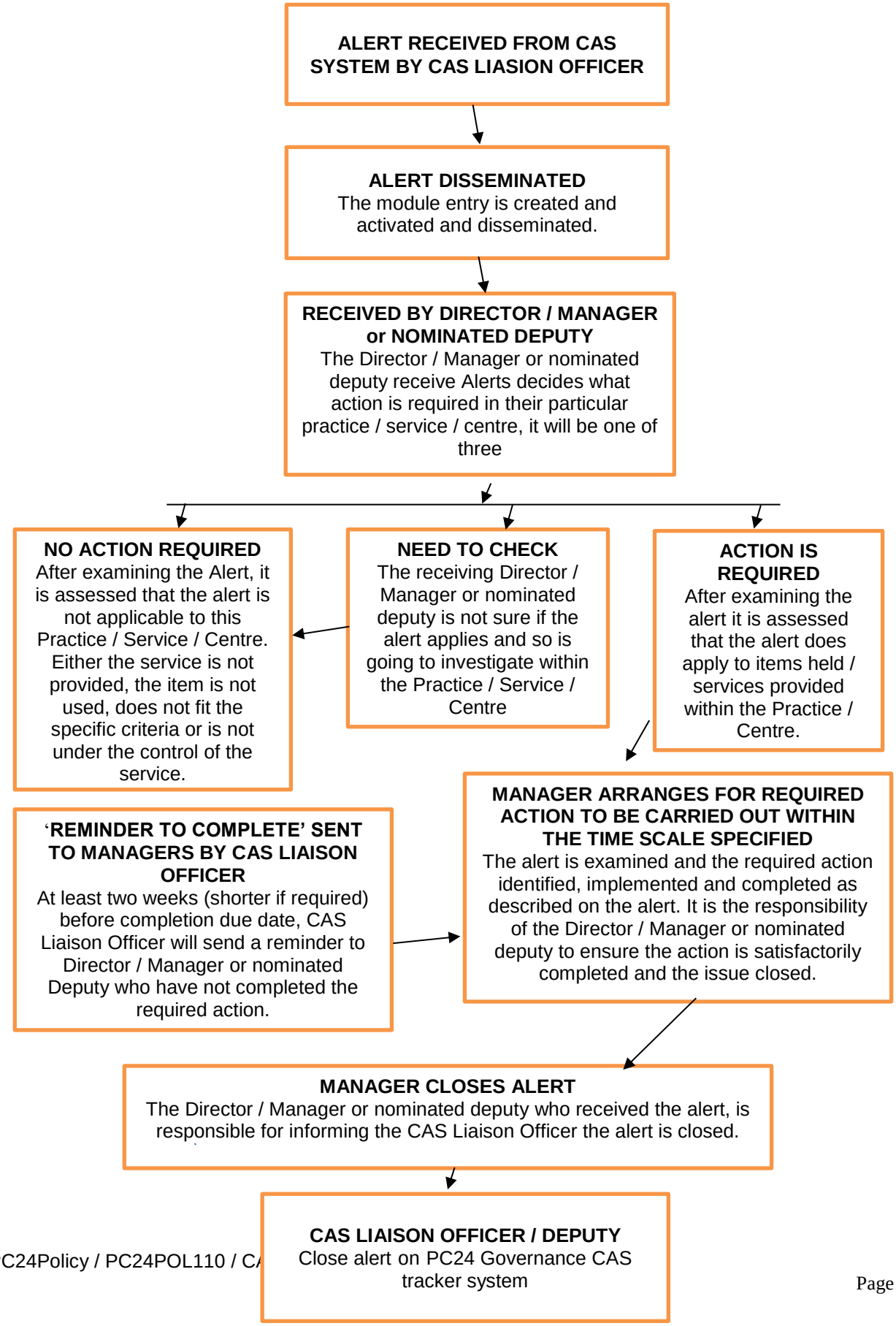
8. Monitoring the effectiveness of the procedure

Minimum requirements to be monitored	Process for monitoring e.g. audit	Responsible individual, group or committee	Frequency of monitoring	Responsible individual, group or committee for review of results	Responsible individual, group or committee for development of action plan	Responsible individual, group or committee for monitoring of action plan
Procedure KPI's are achieved	Monitoring of PC24's Central Alerting Systems – Monthly Alerts	Quality and Workforce	Bi annually	Quality & Workforce Committee	Executive Director of Nursing and Quality / Director Business of Finance	Quality and workforce
Management of PC24 delegated Clinical Alerts	Monitoring of PC24's Central Alerting Systems – Monthly Alerts (Clinical)	Governance Group	Bi annually	Quality & Workforce Committee	Executive Director of Nursing and Quality	Quality and workforce
Audit of the two of the different types of CAS alerts	PC24's Clinical Audit Programme 2017/2018	Clinical Audit & Effectiveness Lead	Annual	Quality & Workforce Committee	Executive Director of Nursing and Quality / Director Business of Finance	Audit Committee
Audit of CAS Alerts Systems and Processes	360 Degree Internal Audit / Audit of Compliance	Clinical Audit & Effectiveness Lead	Every three years, following the first which will be subject to review in October 2018	Quality & Workforce Committee	Executive Director of Nursing and Quality	Audit Committee
Management of on-going actions such as patient follow ups	Monitoring of on-going actions	CAS Liaison Officer	Ongoing	Quality & Workforce Committee	Executive Director of Nursing and Quality	Audit Committee
Monitoring of Estates Facilities Management alerts	Monitoring of status	Health & Safety Lead	Quarterly	Quality & Workforce Committee	Director Business of Finance	Audit Committee

Monitoring performance	Performance Report	Quality & Workforce Committee Service Delivery performance Group	Monthly	Quality & Workforce Committee	Executive Director of Nursing and Quality / Director Business of Finance	Audit Committee

Appendix A

CAS ALERT ACTION FLOW CHART



Appendix B

Equalities and Health Inequalities – Screening Tool

Equalities and Health Inequalities – Screening Tool

Version number: V1

First published: November 2016

To be read in conjunction with Equalities and Health Inequalities Analysis Guidance, Quality & Patient Safety Team, Primary Care 24, 2016.

Prepared by: Quality & Patient Safety Team.

Introduction

The purpose of this Screening Tool is to help you decide whether or not you need to undertake an Equality and Health Inequalities Analysis (EHIA) for your project, policy or piece of work. It is your responsibility to take this decision once you have worked through the Screening Tool. Once completed, the Head of your SDU or the Quality & Patient Safety Team will need to sign off the Screening Tool and approve your decision i.e. to either undertake an EHIA or not to undertake an EHIA.

The Quality and Patient Safety Team can offer support where needed. It is advisable to contact us as early as possible so that we are aware of your project.

When completing the Screening Tool, consider the nine protected characteristics and how your work would benefit one or more of these groups. The nine protected characteristics are as follows:

1. **Age**
2. **Disability**
3. **Gender reassignment**
4. **Marriage and civil partnership**
5. **Pregnancy and maternity**
6. **Race**
7. **Religion and belief**
8. **Sex**
9. **Sexual orientation**

A number of groups of people who are not usually provided for by healthcare services and includes people who are homeless, rough sleepers, vulnerable migrants, sex workers, Gypsies and Travellers, Female Genital Mutilation (FGM), human trafficking and people in recovery. Primary Care 24 will also consider these groups when completing the Screening Tool:

The **guidance** which accompanies this tool will support you to ensure you are completing this document properly. It can be found at: http://extranet.urgentcare24.co.uk/

Equality and Health Inequalities: Screening Tool

A	General information
A1	What is the title of the activity, project or programme? **CAS Alerts Policy**
A2	What are the intended outcomes of this work? Please outline why this work is being undertaken and the objectives. The policy details the arrangements for the receipt, assessment, dissemination and completion of all alerts received from the Central Alerting System (CAS). This is to ensure PC24 has clear and defined arrangements for ➢ The Medicines and Healthcare products Regulatory Agency (MHRA) – Drug Alerts ➢ NHS England ➢ Department of Health (DoH) ➢ NHS Department of Estates and Facilities (EFA) ➢ Patient Safety Alerts (PSA) ➢ Medical Device Alerts (MDA)
A3	Who will be affected by this project, programme or work? Please identify whether the project will affect staff, patients, service users, partner organisations or others. This policy applies to all PC24 staff who are involved in any aspect of internal / external alert dissemination, action and/or review. The content of the communications from the Central Alert System may indirectly impact on patients, this information is directed from DH in order to safeguard patients, visitors and staff from harm.
B	The Public Sector Equality Duty

B1	Could the initiative help to reduce unlawful discrimination or prevent any other conduct prohibited by the Equality Act 2010? If yes, for which of the nine protected characteristics (see above)?		
	Yes	**No**	Do not know
	Summary response and your reasons: The policy describes the details of a corporate function of PC24 and there are no adverse impacts on people with a particular protected characteristic. The content of the communications from the Central Alert System may indirectly impact on patients, this information is directed from DH in order to safeguard patients, visitors and staff from harm.		
B2	Could the initiative undermine steps to reduce unlawful discrimination or prevent any other conduct prohibited by the Equality Act 2010? If yes, for which of the nine protected characteristics?		
	Yes	**No**	Do not know
	Summary response and your reasons: This is a corporate policy and it describes the arrangements within the organisation for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		
B3	Could the initiative help to advance equality of opportunity? If yes, for which of the nine protected characteristics?		
	Yes	No	Do not know
	Summary response and your reasons: This is a corporate policy and it describes the arrangements within the organisation for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		
B4	Could the initiative undermine the advancement of equality of opportunity? If yes, for which of the nine protected characteristics?		
	Yes	**No**	Do not know
	Summary response and your reasons: This is a corporate policy and it describes the arrangements within the organisation for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		
B5	Could the initiative help to foster good relations between groups who share protected characteristics? If yes, for which of the nine protected characteristics?		
	Yes	No	Do not know
	Summary response and your reasons: This is a corporate policy and it describes the arrangements within the organisation for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		
B6	Could the initiative undermine the fostering of good relations between groups who share protected characteristics? If yes, for which of the nine protected characteristics?		
	Yes	**No**	Do not know
	Summary response and your reasons**:** This is a corporate policy and it describes the arrangements for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		
C	**The duty to have regard to reduce health inequalities**		
C1	Will the initiative contribute to the duties to reduce health inequalities?		
	Could the initiative reduce inequalities in access to health care for any groups which face health inequalities? If yes for which groups?		
	Yes	**No**	Do not know
	Summary response and your reasons: This is a corporate policy and it describes the arrangements for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		

C2	Could the initiative reduce inequalities in health outcomes for any groups which face health inequalities? If yes, for which groups?		
	Yes	**No**	Do not know
	Summary response and your reasons: This is a corporate policy and it describes the arrangements for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		
D	Will a full Equality and Health Inequalities Analysis (EHIA) be completed?		
D1	Will a full EHIA be completed? Bearing in mind your previous responses, have you decided that an EHIA should be completed? Please see notes. [1] Please place an X below in the correct box below. Please then complete part E of this form.		
	Yes	Cannot decide	**No**
E	Action required and next steps		
E1	If a full EHIA is planned: Please state when the EHIA will be completed and by whom. Name: Date:		
E2	If no decision is possible at this stage: If it is not possible to state whether an EHIA will be completed, please summarise your reasons below and clearly state what additional information or work is required, when that work will be undertaken and when a decision about whether an EHIA will be completed will be made. Summary reasons: Additional information required: When will it be possible to make a decision about an EHIA?		
E3	If no EHIA is recommended: If your recommendation or decision is that an EHIA is not required then please summarise the rationale for this decision below. Summary reasons: This is a corporate policy that describes the arrangements within the organisation for the management alerts received from the DH's central alerting system. The policy applies equally to relevant staff with responsibilities as documented in the policy.		

F	*Record Keeping*		
Lead originator:	Sheila Dineley	Date:	31/08/2017

[1] Yes: If the answers to the previous questions show the PSED or the duties to reduce health inequalities are engaged/in play a full EHIA will normally be produced. No: If the PSED and/or the duties to reduce health inequalities are not engaged/in play then you normally will not need to produce a full EHIA.

Director signing off screening:	Mary Ryan	Date:	31/08/2017
Directorate:	Quality & Patient Safety	Date:	31/08/2017
Screening published:		Date:	

Appendix C

Privacy Impact Assessment

Data Protection Act 2018
PRIVACY IMPACT ASSESSMENT (PIA)
CAS Alerts Policy

Compliance Checklist

Privacy

Privacy has become a much larger consideration for business and government in recent years. New information technologies have increased public concerns about intrusion into their privacy.

Beyond the recognition of privacy as a human right, specific laws have been introduced to deal with particular areas of concern. Much of the legislative attention to date has been focused on information about people that is collected, stored, used and disclosed by organisations. The handling of personal data is regulated by the Data Protection Act 1998, which the Information Commissioner's Office oversees.

Privacy impact assessment

Privacy Impact Assessment (PIA) is a process which enables organisations to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset that reduces privacy intrusion.

This Privacy Impact Assessment (PIA) aims to assist Primary Care 24 when proposing change to investigate whether the personal information aspects of their project comply with the data protection principles in Schedule 1 of the Data Protection Act (DPA).

The checklist has been designed for use by any employee proposing change. The Quality & Patient Safety Team should be consulted about the completion of this checklist.

It should be noted that many terms used in the **principles** have meanings specific to the **Data Protection Act**, and it would be prudent to refer to the Act for definition for those terms. Another useful reference is the specific guidance on the Information Commissioner's website **https://ico.org.uk/**

A) BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1 Lead Directorate and project name	
Directorate	Quality & Patient Safety
Department	Governance
Project	Communication of Safety Alerts and Safety Critical Information (Central Alerting System) Policy

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 the PIA questions)	
Name	Sheila Dineley
Title	Governance Administrator
Phone Number	0151 254 1553
E-Mail	Sheila.dineley@PC24.nhs.uk

3 Description of the programme / system / technology / legislation (initiative) being assessed.
If this is a change to an existing project, system, technology or legislation, describe the current system or programme and the proposed changes. *(N.B. if the initiative does **not** collect, use or disclose personal data* - see definition and statement below).*

4 Purpose / objectives of the initiative (if statutory, provide citation/reference).	
Purpose	The purpose of this policy is to detail the PC24 arrangements for the receipt, assessment, dissemination and completion of all alerts received from the CAS system.

5 What are the potential privacy impacts of this proposal?
Nil. See section C.

IF THERE IS NO PERSONAL DATA INVOLVED,
GO STRAIGHT TO SECTION 'C' DPA COMPLIANCE - CONCLUSIONS (on the last page)

***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.

(Data Protection Act, section 1)

B) DATA PROTECTION PRINCIPLES (DPPs)

PRINCIPLE 1 FAIR AND LAWFUL PROCESSING	
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met	
1.1 Preliminary	
What type of personal data are you processing?	
1.2 Schedule 2 Conditions relevant for purposes of the first principle: processing of any personal data	
Describe the purposes for which you will be processing personal data.	
List which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data.	
1.3 Schedule 3 Conditions relevant for purposes of the first principle: processing of any *sensitive* personal data	
If this project does not involve the processing of sensitive personal data, please go to section 1.4	
Identify the categories of *sensitive personal data* that you will be processing.	

Identified *the purposes* for which you will be processing *sensitive personal data*.	
Identify which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing *sensitive personal data*?	
1.4 Obtaining consent	
Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?	Delete as appropriate Yes No
If yes, when and how will that consent be obtained?	.
For the processing of *sensitive personal data*, are you relying on *explicit* consent as specified in Schedule 3, s1 of the Data Protection Act?	Delete as appropriate Yes No
If yes, when and how will that consent be obtained?	
1.5 Lawful processing	
How is compliance with the Human Rights Act being assessed?	Via this PIA Review and the Data Sharing Agreement - Information is limited to a need to know and informed consent is provided to ensure no breach of Human Rights occurs.
Are you assessing whether your processing is subject to any other legal or regulatory duties?	Delete as appropriate Yes No
If yes, how is that assessment being made? If no, please indicate why not.	
1.6 Fair processing	
How are individuals being made aware of how their personal data is being used?	
How individuals are offered the opportunity to restrict processing for other purposes?	
When is that opportunity offered?	
1.7 Exemptions from the first data protection principle	
The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair *Data Protection Act:* ***https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions***	
Do you provide individuals with all of the information in the box above?	Delete as appropriate Yes No

If no, which exemption to these provisions is being relied upon?		
PRINCIPLE TWO: THE PURPOSE OR PURPOSES FOR PROCESSING PERSONAL DATA		
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.		
2.1 Use of personal data within the organisation		
What procedures are in place for maintaining a comprehensive and up-to-date record of use of personal data?		
Is any data processing carried out on your behalf (e.g. by a subcontractor)?	Delete as appropriate Yes No	
If yes, please identify		
2.2 Use of existing personal data for new purposes		
Does the project involve the use of existing personal data for new purposes?	Delete as appropriate Yes No	
If no, go to section 2.3		
If yes, How is the use of existing personal data for new purposes being communicated to:- *a) the data subject:* b) *the Data Protection Officer (responsible for Notification)*	a)	
	b)	
2.3 Disclosure of data		
How individuals / data subjects are made aware of disclosures of their personal data?		
PRINCIPLE 3: ADEQUACY AND RELEVANCY		
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.		
3.1 Adequacy and relevance of personal data		
How is the *adequacy* of personal data for each purpose determined?		
How is an assessment made as to the *relevance* (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?		
What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?		
PRINCIPLE 4: ACCURATE AND UP TO DATE		
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.		
4.1 Accuracy of personal data		
How often is personal data being checked for accuracy?		
How is the accuracy of the personal data being checked with the Data Subject?		
4.2 Keeping personal data up to date		

How is personal data evaluated to establish the degree of damage to: (a) the data subject or (b) the data controller that could be caused through being out of date?	a)	
	b)	
PRINCIPLE 5 NO LONGER THAN NECESSARY		
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.		
5.1 Retention policy		
Is the project subject to any statutory / sectorial requirements on retention?	Delete as appropriate Yes No	
If yes please state relevant requirements		
5.2 Review and deletion of personal data		
When data is no longer necessary for the purposes for which it was collected: a) How is a review made to determine whether the data should be deleted? b) How often is the review conducted? c) Who is responsible for determining the review? d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?	a)	
	b)	
	c)	
	d)	
If yes, please explain		
Are there any exceptional circumstances for retaining certain data for longer than the normal period?	Delete as appropriate Yes No	
If yes, please provide justification		
PRINCIPLE 6 SUBJECTS RIGHTS/SUBJECT ACCESS		
Personal data shall be processed in accordance with the rights of data subjects under this Act.		
6.1 Subject access		
How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?		
6.2 Withholding of personal data in response to a subject access request		
Are there any circumstances where you would withhold personal data from a subject access request?	Delete as appropriate Yes No	
If yes, on what ground. If no, go to 6.3		
How are the grounds for doing so identified?		

If yes, please provide justification	
6.3 Processing that may cause damage or distress	
Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?	Delete as appropriate Yes No
If yes, please specify proposed procedures. If no, please indicate why not.	
Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?	Delete as appropriate Yes No
If yes, please explain	
6.4 Right to object	
Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	Delete as appropriate Yes No N/A Other
If yes, please explain	

6.5 Automated decision	
Are any decisions affecting individuals made solely on processing by automatic means?	Delete as appropriate Yes No
If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?	
6.6 Rectification, blocking, erasure and destruction	
What is the procedure for responding to data subject's notice (in respect of accessible records) or a court order requiring: a) rectification; b) blocking; c) erasure or; d) destruction of personal data?	a)
	a)
	b) .
	c)
PRINCIPLE 7 SECURITY OF PERSONAL DATA	
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
7.1 Security Policy	
Is the level of security appropriate for the type of personal data processed?	Delete as appropriate Yes No
If yes please explain	
7.2 Unauthorised or unlawful processing of data	
Describe security measures that are in place to prevent any unauthorised or unlawful processing of: a) Data held in an automated format e.g. password controlled access to PCs b) Data held in a manual record e.g. locked filing cabinets	a)
	b)
Is there a higher degree of security to protect *sensitive personal data* from unauthorised or unlawful processing?	Delete as Appropriate Yes No
If yes, please describe the planned procedures. If no, please indicate why not.	
Describe the procedures in place to detect breaches of security (remote, physical or logical)? **logical (such as hacking etc)*	

7.4 Destruction of personal data		
Describe the procedures in place to ensure the destruction of personal data no longer necessary?		
7.5 Contingency planning		
Is there a contingency plan to manage the effect(s) of an unforeseen event?	Delete as Appropriate Yes No	
If yes, please give details		
Describe the risk management procedures to recover data (both automated and manual) which may be damaged/lost through: a) human error b) computer virus c) network failure d) theft e) fire f) flood g) other disaster.	a)	.
	b)	
	c)	
	d)	
	e)	
	f)	
	g)	
7.6 Choosing a data processor		
How do you ensure that the Data Processor complies with these measures?		
PRINCIPLE 8 OVERSEAS TRANSFER (OUTSIDE OF THE EEA)		
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.		
8.1 Adequate levels of protection		
Are you transferring personal data to a country or territory outside of the EEA[2]? [1] The European Economic Area (EEA) comprises the 27 EU member states plus Iceland, Liechtenstein and Norway.	Delete as appropriate Yes No	
If no, go to Part III If yes, where?		
What types of data are transferred? (e.g. contact details, employee records)		
Are *sensitive personal data* transferred abroad?	Delete as appropriate Yes No	
If yes, please give details		
Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	Delete as appropriate Yes No	
If yes, please describe. If no, please indicate why not.		
Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	Delete as appropriate Yes No	

If yes, please give details	

C) DATA PROTECTION PRINCIPLES COMPLIANCE - CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the Data Protection Principles. This could include indicating whether some changes or refinements to the project might be warranted.

Corporate policy that contains no personal or sensitive information.

IG Manager Name: Margaret Swinson

IG Manager Signature:

Date: 07.11.2017

Project Manager: Sheila Dineley

Project Manager Signature: Sheila Dineley

Date: 07.11.2017