Health Informatics Centre
University of Dundee

HIC SERVICES STANDARD OPERATING PROCEDURE

Handling Significant Events

SOP NUMBER:	HIC Services SOP 03
VERSION NUMBER:	5.0
EFFECTIVE DATE:	15th November 2022
DOCUMENT SECURITY LEVEL:	Open
REVIEW DATE:	This SOP will be reviewed at least every 12 months, or at other times as requested by: HIC Information Governance Committee
AUTHOR:	Duncan Heather
DATE APPROVED BY HIC INFORMATION GOVERNANCE COMMITTEE:	15/11/2022
DATE APPROVED BY HIC EXECUTIVE COMMITTEE:	14/01/2020
DATE REVIEWED BY HIC OPERATIONS GROUP:	N/A
CONTACT PERSON FOR THIS SOP:	HIC Information Security and Governance Manager

DOCUMENT REVIEW AND REVISION HISTORY:

Version Number:	Edited by (job title):	Effective Date:	Details of editions made:
1.0	Duncan Heather (HIC Governance Manager)	01/09/13	This is a new SOP which expands on a subset of policies and supersedes Version 6 of the HIC Standard Operating Procedure, Management of HIC Datasets. Effective from 1st August 2011.
1.1	Duncan Heather (HIC Governance Manager)	15/05/14	Add diagram of Governance Reporting Structure
2.0	Duncan Heather (HIC Governance Manager)	01/01/15	Revise Governance reporting to include TASC
3.0	Duncan Heather (HIC Governance Manager)	01/01/16	Added contact matrix at 5.1.1.7
4.0	Duncan Heather (HIC Governance Manager)	08/11/18	Extensively updated, adding GDPR details relating to reporting potential breach to Information Commissioner's Office
5.0	Duncan Heather (HIC Governance Manager)	31/01/2020	Updated at the request of the Information Governance Committee, to remove any ambiguity about how a Significant Event is identified and when it should be escalated to UoD DPO. Revised flowchart 5.2.1.8

	Rachael Torano (Business Support)	14/05/2020	Updated with new and approved Header Changes made to cover page to include Op's review date as agreed at the HIC Information Governance Meeting Document Review and Revision History header updated As agreed by the HIC Governance Committee signatures have been removed from cover page and Document Review and Revision History table has been updated to include review dates and notes
5.0	Jenny Johnston	15/11/2022	Reviewed process and no updates required

Draft and Archived/Obsolete revisions are not to be used.
Access current versioning system to verify revision.

1. PURPOSE

Health Informatics Centre Services (HIC Services) is a University Research Support Unit operating within the TAyside medical Science Centre (TASC) at the University of Dundee, in collaboration with NHS Tayside and NHS Fife. HIC Services provides Data Users with linked, anonymised information derived mostly from large Population Based Health Datasets, owned mainly by the NHS and the University of Dundee. HIC also develops data collection software, provides data entry and securely hosts data for research use.

This SOP describes procedures to follow when unexpected events occur when processing or using Data provided by HIC Services, including:

- Reporting significant events
- Reporting a Business Continuity Plan incident
- Reporting potential data breaches to the Information Commissioner's Office (ICO)
- Responding to analyses that raise potential NHS Clinical Governance, criminal or reputational issues

2. SCOPE

This SOP covers all of the projects and tasks which HIC undertake. It is applicable to all HIC staff. This SOP will be made available to all users and potential users of the HIC Service and will be externally visible on the public HIC website.

3. DEFINITIONS

For overall Definitions see HIC Services SOP Appendix B –Definitions.

- **Personal data breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

4. RESPONSIBILITIES

- HIC Director – Responsible for overall HIC security policy and implementation
- Process Manager – Ensuring SOPs are followed by team
- Governance Manager – Monitoring compliance, handling significant events, keeping SOP up to date, responding timeously to a reportable potential data breach. In absence of Governance Manager, a deputy will be appointed by the HIC Manager
- All HIC Staff – Responsible for adherence to the SOP as specified

5. POLICY

For overall Policy see HIC Security Policy and HIC Services SOP Appendix A – Policy.

5.1 Identifying Significant Events

5.1.1.1 A Significant Event is defined as a significant deviation from the terms of HIC Information Security Management System (ISMS) documented policies and processes, or other event that creates a risk to HIC data security. HIC requires all staff and Approved Data Users to report all Significant Events, to enable processes to be improved.

5.2 Reporting Significant Events

5.2.1.1 Contact your line manager and the HIC Governance Manager in the first instance to report any incident that might be considered a significant event.

5.2.1.2 At this point, the event will be reviewed and, if a Significant Event has taken place, assigned one of the following categories by the Governance Manager. The Governance Manager will assess any potential use of data and the likelihood and severity of the resulting risk to the data subject's rights and freedoms.

Category 1 - Deviation from HIC ISMS documentation, with no data involved. A Significant Event Assessment (SEA) report will be completed.

Category 2 - - A personal data breach has occurred with no, or low, resulting risk to data subject(s) rights and freedoms. The event is considered unlikely to result in a significant risk to data subject(s) so there is no requirement to report to the ICO, however, the reasons for not doing so will be included within the SEA report. A copy of the finalised report will be sent to the University Data Protection Officer (DPO).

Category 3 - A personal data breach has occurred with high resulting risk to data subject(s). The Governance Manager will immediately notify the HIC Manager, HIC Director, Data Controller and University DPO and TASC Director to discuss and confirm the likely need to notify the ICO. Any ICO notification needs to be done within 72 hours of initially becoming aware of the significant event. An initial report will need to be prepared within 24 hours, following section "**Reporting a Data Breach to ICO**" below.

5.2.1.3 The HIC Governance Manager, in collaboration with HIC staff directly involved, will initiate a HIC Significant Event Analysis (SEA) report, containing information about the incident, along with any solutions implemented, in the following format:

- What happened?
- How did it happen?
- Severity Category
- Reason the event is/is not considered a reportable breach
- Lessons learnt
- Action Timelines
- Training Requirements Identified

5.2.1.4 The report will be submitted to the TASC Senior Clinical Research Governance Manager.

5.2.1.5 The report will also be submitted to the HIC Executive Committee where a decision can be taken as to whether any further action is necessary. When the event is deemed to be serious HIC will notify the chair of the HIC Governance Committee without waiting to report at the next HIC Governance Committee Meeting to report on the event. Resulting actions will be tracked until completion at the HIC Executive Committee.

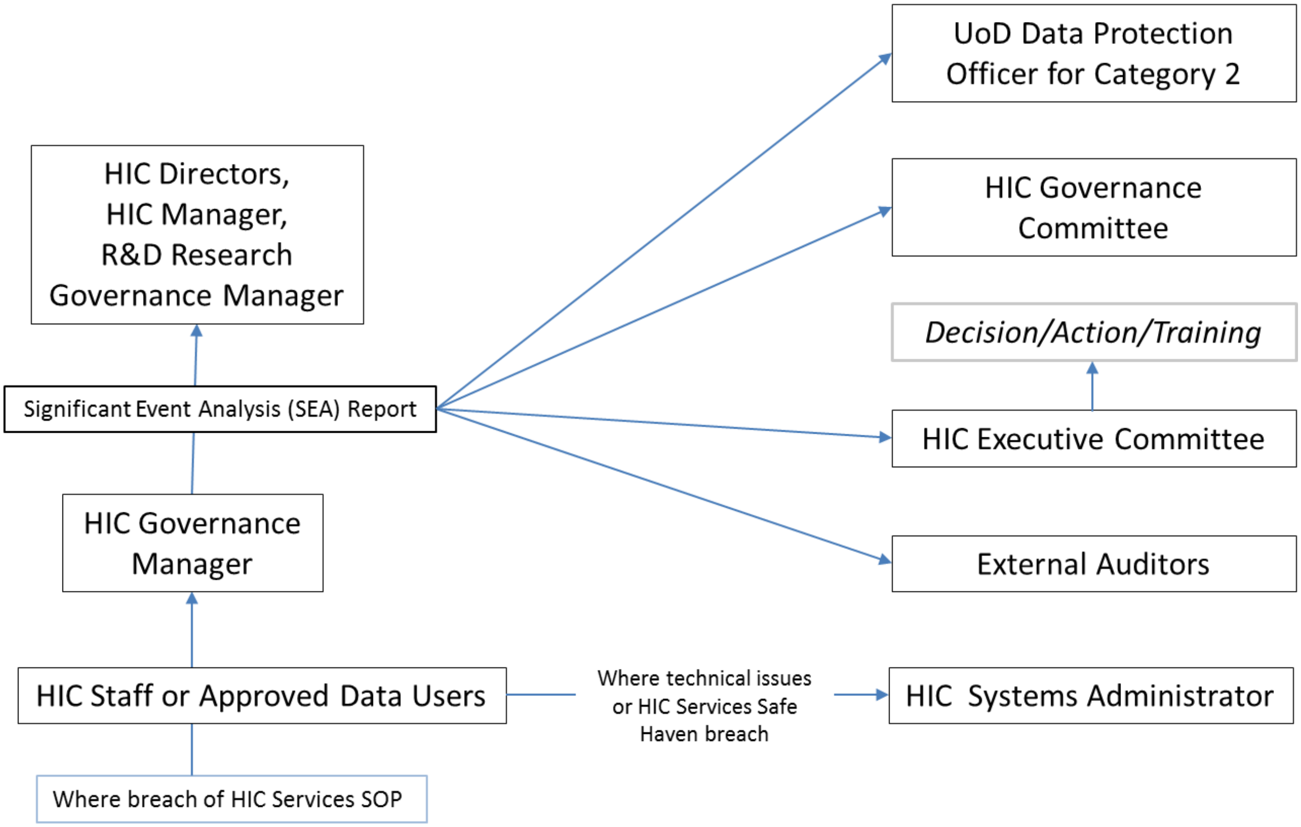
5.2.1.6 All events will be reported to the HIC Governance Committee at the next meeting, the annual auditors and will be added to the Project Management System (PMS).

5.2.1.7 If a Significant Event is identified in relation to a technical issue or HIC Services Safe Haven breach the System Administrator should be notified immediately, who would assess the severity of the issue and take one of three courses of action:

- Suspend all use of the HIC Services Safe Haven, or any other affected part of HIC IT Systems or Infrastructure, until investigation is completed.

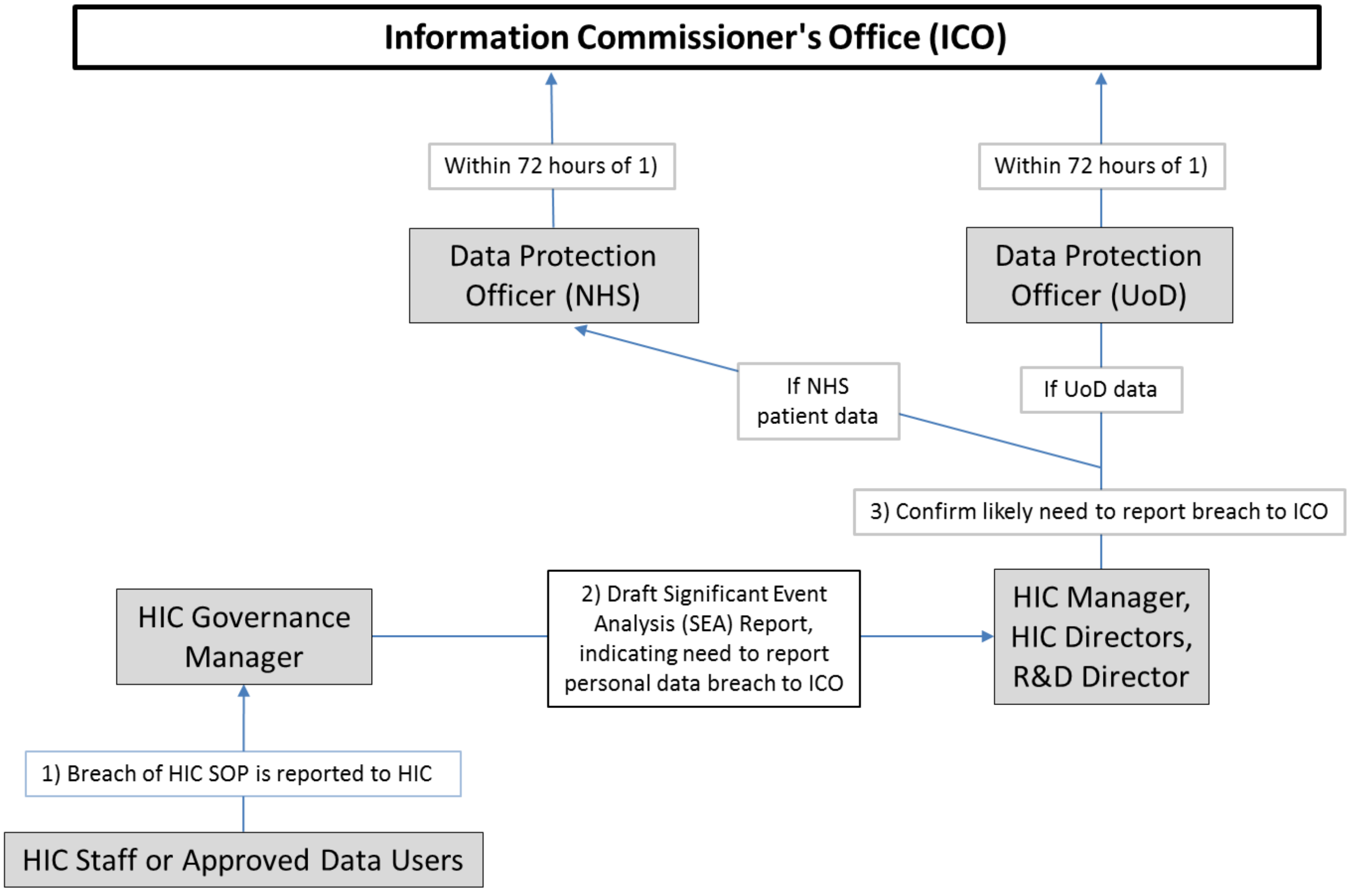
- Suspend only those HIC Technical staff or Approved Data Users who are part of the Project Group under investigation.
- Do nothing and monitor use whilst investigating the Significant Event.

5.2.1.8 See diagram below for illustrating how significant events are escalated.


UoD Data Protection Officer for Category 2
HIC Directors, HIC Manager, R&D Research Governance Manager
HIC Governance Committee
Decision/Action/Training
Significant Event Analysis (SEA) Report
HIC Executive Committee
HIC Governance Manager
External Auditors
HIC Staff or Approved Data Users
Where technical issues or HIC Services Safe Haven breach
HIC Systems Administrator
Where breach of HIC Services SOP

Depending on the nature of the event and, for example, which Data Controller is affected, refer to the HIC Event Contact list in the HIC Business Continuity Plan (BCP).

5.3 Reporting a Category 3 Personal Data Breach to the Information Commissioner's Office (ICO)


Information Commissioner's Office (ICO)
Within 72 hours of 1)
Within 72 hours of 1)
Data Protection Officer (NHS)
Data Protection Officer (UoD)
If NHS patient data
If UoD data
3) Confirm likely need to report breach to ICO
HIC Governance Manager
2) Draft Significant Event Analysis (SEA) Report, indicating need to report personal data breach to ICO
HIC Manager, HIC Directors, R&D Director
1) Breach of HIC SOP is reported to HIC
HIC Staff or Approved Data Users

5.3.1.1 The TASC Director and HIC Directors will ultimately make the decision to escalate the event to the Data Protection Officer of the University or NHS for potential reporting to the ICO.

5.3.1.2 In the event of an NHS data breach, the UoD Data Protection Officer will be kept informed, while the NHS Data Protection Officer will be responsible for reporting to the ICO.

5.3.1.3 The Governance Manager will provide sufficient initial information about the breach, within the SEA, to enable an effective and prompt initial ICO report to the Data Controller Data Protection Officer, within 24 hours:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description, as much as possible at this early stage, of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5.3.1.4 The HIC Governance Manager will advise and keep track of the 72 hour reporting deadline as the reporting process progresses, to help ensure this is met.

5.4 Responding to analyses that raise potential NHS Clinical Governance, criminal or reputational issues

5.4.1.1 Analyses for academic purposes may identify care which raises concerns about patient safety, broader clinical governance or the reputation of particular professionals, institutions or whole systems of care. Additionally if any prima facie indications of malicious or potentially fraudulent or otherwise criminal activity associated (directly or indirectly) with the study are uncovered during the course of the study, those concerned need to act with speed and in confidence, taking actions that are in proportion to the size and severity of the suspected risk and consider legal risks such as defamation and a court's ability to demand records. HIC Services has limited resources to investigate such issues and it will usually be most appropriate for HIC Services to confine its role to alerting the NHS Medical Director to a potential problem and suggesting how this might be investigated. However, in circumstances suggesting risk to individuals or organisations, everyone using HIC Services Data has an obligation to alert senior HIC Services staff who will in turn promptly alert the Medical Director within the relevant Health Board in the first instance, if there are serious grounds for concern.

5.4.1.2 If an Approved Data User believes that their analysis raises such concerns, then they should initially report them in confidence to the HIC Governance Manager or HIC Data Analyst, who will ensure that they are rapidly considered by a senior clinical member of the HIC Executive Committee who is independent of the project. If necessary, the Senior Clinical member of the HIC Executive Committee may consult others confidentially on the implications of the analysis, for example drawing on specialist expertise, to inform a decision about whether the analysis suggests a problem that requires action by HIC Services and/or the NHS. It is not possible to pre-specify all situations, but they are likely to fall into one of these classifications:

- No Clinical Governance issues identified, or minor issues
- Significant Clinical Governance issues identified
- Significant issues AND risk to patients, or likely to cause damage or distress

5.4.2 Actions – Clinical member of HIC Exec

5.4.2.1 Decision that there is no significant clinical governance or reputational issue identified:

- Document the rationale for the decision

5.4.2.2 Decision that there is a potential quality of care, criminal or reputation issue identified, but that no immediate risk to patients exists:

- Notify Medical Director within the relevant Health Board giving 30 days' notice prior to publication
- Document the rationale for the decision

5.4.2.3 Decision that there is the potential for a high risk, patient safety, criminal or reputational issue to arise (likely to be rare):

- Urgently notify the Medical Director within the relevant Health Board that in the opinion of the HIC Executive Committee member, there is a potential risk to patients or reputation
- If necessary, and if HIC Services resources allow, HIC Services to work with the relevant Health Boards to ascertain whether further analysis would be helpful before NHS action (e.g. since many analyses do not use the most current data, consider whether the analysis needs to be repeated in more recent data; consider whether de-anonymisation is required to identify patients needing intervention)
- Support Health Board action in monitoring the effects of any intervention, if HIC Services resources allow
- Document the rationale for the decision

5.4.2.4 All documentation to be stored on the PM System by the HIC Governance Manager and the incident reported to the HIC Governance Committee.

6. APPLICABLE REFERENCES

- HIC Services SOP 01 HIC Data Security
- HIC Services SOP 02 Data Access Approvals
- HIC Services Staff Confidentiality Agreement
- HIC Services Data User Agreement
- HIC Services SOP Appendix A – Policy
- HIC Services SOP Appendix B – Definitions
- HIC Services SOP Appendix C – Roles and Contact Details
- HIC Business Continuity Plan (BCP)