|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: | **OFFICIAL**  **NHS Digital - Higher Severity Service Incident Management Process** | | |
| Project / Programme | **Service Management** | Project | **Service Operations** |
| Document Reference | **NHS Digital-0046-488** | | |
| Project Manager | **Fraser Fearn** | Status | **FINAL** |
| Owner | **Pete Tebay** | Version | **6.9** |
| Author | **Pete Tebay** | Version issue date | **20/07/2020** |

**NHS Digital Higher Severity Service Incident Management Process**

Document management

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| 0.1 | 09/02/06 | First draft |
| 0.2 | 08/06/06 | Added lower-level details |
| 0.3 | 20/10/06 | Amended details |
| 0.4 | 24/11/06 | Amended NHS Digital contact details |
| 0.5 | 18/12/06 | Amended NHS Digital contact details |
| 0.6 | 31/08/07 | Full process and document review |
| 0.7 | 19/10/07 | Service Management General Review |
| 1.2 | 23/09/08 | PID information update |
| 1.3 | 10/10/08 | Updated new communications policy information. |
| 1.4 | 09/12/08 | Updated State of the Nation Process |
| 1.5 | 28/05/09 | Update sections in line with the new comms policy. |
| 2.0 | 28/05/09 | Updated Owner & Author information. |
| 2.1 | 16/12/09 | Updated security process |
| 2.2 | 29/01/10 | Updated escalation process |
| 3.0 | 22/03/10 | Full review of HSSI process |
| 3.1 | 04/06/10 | Updated with NSD out of hours changes |
| 4.0 | 03/07/10 | Above changes confirmed signed off |
| 4.0 | 03/08/11 | In hours HSSI process flow re-written |
| 4.0 | 11/06/12 | End Point disablement process added |
| 4.1 | 24/10/12 | Inputs & Outputs added |
| 4.2 | 05/12/12 | Full process and document review & re-write |
| 5.0 | 05/12/12 | Full process and document review & re-write final |
| 6.0 | 06/09/12 | Updated for full operational activities |
| 6.1 | 01/06/15 | Updated Clinical Incident process |
| 6.2 | 25/05/16 | Updated Endpoint disablement section |
| 6.3 | 17/07/16 | Updated Endpoint disablement section, removed Accenture HSSI section & general tidy up |
| 6.4 | 14/09/16 | Rebranded and reviewed |
| 6.5 | 08/09/17 | Uplifted embedded docs & links to the central store. Core hour change |
| 6.6 | 15/08/18 | Minor updates |
| 6.7 | 19/11/19 | Minor updates to Clinical Incident process |
| 6.8 | 28/11/19 | Appendix review – embedded documents updated |
| 6.9 | 20/04/20 | Updated Service Bridge phone number 0300 303 4333 |

Reviewers

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| Tim Vause | Service Delivery Manager | 23/10/2013 | 6.0 |
| Pete Tebay | Service Management Lead Service Operations | 15/08/2018 | 6.6 |
| Neil Bennett | Head of Service Management | 23/10/2013 | 6.0 |
| Fraser Fearn | Service Management Lead GP & Pharmacy | 23/10/2013 | 6.0 |
| Lyn Marsh | Service Management Lead |  | 6.0 |
| David Miller | NHS Digital Service Desk Team Manager |  | 6.0 |
| Emma Murphy | Environments System Integration Manager | 23/10/2013 | 6.0 |
| Ash Raines | Core Development Programme Manager | 23/10/2013 | 6.0 |
| Mike Anderson | Senior Safety Engineer | 23/10/2013 | 6.0 |
| Dan Taylor | Head of Infrastructure Security |  | 6.0 |

Approved by

This document must be approved by the following people:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title | Date | Version |
| Pete Tebay | Service Management Lead - Service Operations |  | 15/08/2018 | 6.6 |
|  |  |  |  |  |

Glossary of Terms

|  |  |
| --- | --- |
| Term / Abbreviation | What it stands for |
| HSSI | High Severity Service Incident |
| ECAB | Emergency Change Advisory Board |
| ERFC | Emergency Request for Change |
| HSIR | High Severity Incident Report |
| NHS Digital | National Health Service Digital |
| NSP | National Service Provider |
| NCAB | National Change Advisory Board |
| RFC | Request For Change |
| MIM | Major Incident Manager (Manages HSSIs) |
| ITSCM | IT Systems Crisis Management |

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

[1 Introduction 7](#_Toc31273213)

[1.1 Purpose 7](#_Toc31273214)

[1.2 Scope 7](#_Toc31273215)

[1.3 Governance 7](#_Toc31273216)

[1.4 Objectives 7](#_Toc31273217)

[1.5 Background 8](#_Toc31273218)

[2 Invocation of a Higher Severity Service Incident 8](#_Toc31273219)

[3 Higher Severity Service Incident Management Process (Core hours) 10](#_Toc31273220)

[3.1 Process Definition Details 11](#_Toc31273221)

[4 Higher Severity Service Incident Management Process (Out of hours) 14](#_Toc31273222)

[4.1 Process Definition Details 15](#_Toc31273223)

[5 HSSI Types 18](#_Toc31273224)

[5.1 Security Incidents 18](#_Toc31273225)

[5.2 Security Incident Management 18](#_Toc31273226)

[5.3 Patient Identifiable Data (PID) 19](#_Toc31273227)

[5.4 Clinical Safety Incidents 19](#_Toc31273228)

[6 NHS Digital Service Bridge Key Inputs & Outputs 21](#_Toc31273229)

[7 Roles and Responsibilities 21](#_Toc31273230)

[7.1 NHS Digital Service Bridge (In Hours) 21](#_Toc31273231)

[7.2 NHS Digital National Service Desk (Acting as service Bridge Out of Hours) 22](#_Toc31273232)

[7.3 Escalation & Deployment Manager 22](#_Toc31273233)

[7.4 NHS Digital National Service Desk, Accredited Service Desks and other internal Service Desks 23](#_Toc31273234)

[7.5 Service Provider Obligations 23](#_Toc31273235)

[7.6 GPIT Service Provider Obligations 23](#_Toc31273236)

[7.7 NHS Digital Internal Support Teams / Resolver Groups 25](#_Toc31273237)

[8 State of the Nation Process 25](#_Toc31273238)

[9 Communication 25](#_Toc31273239)

[9.1 Programme Director Communications 27](#_Toc31273240)

[9.2 Management Only Communications 27](#_Toc31273241)

[9.3 Early Life Support Communications 27](#_Toc31273242)

[10 Escalation 28](#_Toc31273243)

[11 End Point Disablement 28](#_Toc31273244)

[12 Change Management 29](#_Toc31273245)

[13 NHS Digital Service Management Handovers 30](#_Toc31273246)

[13.1 Service Bridge 30](#_Toc31273247)

[13.2 NHS Digital National Service Desk 30](#_Toc31273248)

[13.3 NHS Digital Escalation & Deployment Manager 30](#_Toc31273249)

[14 HSSI Reporting 31](#_Toc31273250)

[14.1 Higher Severity Service Incident Report 31](#_Toc31273251)

[14.2 HSSI Action Plan 31](#_Toc31273252)

[14.3 Management Summary Report 31](#_Toc31273253)

[15 Post Incident Review 32](#_Toc31273254)

[16 Appendix 33](#_Toc31273255)

[16.1 Appendix A 33](#_Toc31273256)

[16.2 Appendix B 33](#_Toc31273257)

[16.3 Appendix C 33](#_Toc31273258)

[16.4 Appendix D 33](#_Toc31273259)

[16.5 Appendix E 34](#_Toc31273260)

[16.6 Appendix F 34](#_Toc31273261)

[16.7 Appendix G 34](#_Toc31273262)

[16.8 Appendix H 34](#_Toc31273263)

[16.9 Appendix I 34](#_Toc31273264)

# Introduction

## Purpose

This document describes the process details for NHS Digital Service Management in the event of a Higher Severity Service Incident (HSSI) being invoked 24x7x365.

## Scope

This document details the processes to be followed by the NHS Digital Service Bridge team, NHS Digital National Service Desk, and out of hours Escalation & Deployment Managers within the NHS Digital Service Management team and Systems and Service Delivery team.

This document also details the inputs and outputs required from Service Provider organisations, other Service Desks which support internal services and internal NHS Digital support teams to ensure NHS Digital Service Bridge operational activities can be fulfilled.

HSSIs relating to National Services & Applications (internally and externally delivered), Local Service Providers and GPSoC will be managed by the NHS Digital Service Bridge, NHS Digital National Service Desk, other Service Desks which support internal services, internal and external NHS Digital Service Providers and out of hours Escalation & Deployment Managers as per the process documented. This process does not cover the management of HSSIs for Locally Contracted Providers (LCPs) or Existing Service Providers (ESPs) as they are outside of the remit of the NHS Digital Service Bridge. The exception to this is where the issues LCPs/ESPs are experiencing impact on the delivery of NHS Digital managed services.

## Governance

NHS Digital Service Management has the responsibility to manage service delivery, ensuring that the services are being delivered as agreed, to the required level of performance and quality. As part of this Service Integration and Management remit there are instances where NHS Digital Service Management has to co-ordinate the activities of the internal and external NHS Digital Service Providers to ensure that service quality is not compromised and that any risks to clinical (patient) safety, security or information governance (IG) are reduced or avoided.

## Objectives

The objective of the HSSI Management process is to bring additional management expertise and focus to the HSSI, with the authority to lever whatever resources are required to resolve the Incident in the fastest possible time. This is a collaborative process between the NHS Digital Service Bridge Team/NHS Digital National Service Desk, other Service Desks which support internal services, internal and external NHS Digital Service Providers and Escalation & Deployment Managers, with the primary objective of minimising the impact of an HSSI to the user community.

## Background

The NHS Digital Service Bridge team are part of NHS Digital National Service Management with Operations and Assurance Services. The NHS Digital Service Bridge monitor, manage and communicate HSSIs (severity 1 and 2 incidents) and are on site at the Whitehall building, Leeds from 08.00 – 17.30 Mon-Fri excluding bank holidays. The NHS Digital Service Bridge team provides an operational and governance role to all suppliers of NHS Digital services in the event of a HSSI.

Out of hours HSSI Management is performed by the NHS Digital National Service Desk and out of hours Escalation & Deployment Managers on a rotation basis. The Escalation & Deployment Manager is not necessarily a member of the NHS Digital Service Bridge team, but is a member of NHS Digital Service Management.

# Invocation of a Higher Severity Service Incident

The ITIL (Information Technology Infrastructure Library) term for a HSSI is Major Incident and it also states:

A separate [procedure](javascript:void(0)), with shorter timescales and greater urgency, must be used for ‘major’ [incident](javascript:void(0))s. A definition of what constitutes a [major incident](javascript:void(0)) must be agreed and ideally mapped onto the overall incident prioritization scheme – such that they will be dealt with through this separate procedure.

Within NHS Digital the definition of a Higher Severity Service Incident is a severity 1 or 2 incident, which may be caused by:

* Outage or significant performance issues affecting multiple local sites.
* Outage or significant performance issues affecting National systems and services.
* A clinical safety risk identified following assessment by NHS Digital or a supplier organisation.
* A security / information governance risk assessed as medium / high risk by NHS Digital or a supplier organisation.

For the NHS Digital Severity Level Guidelines please see the [appendix](#_Appendix_H).

The impact and urgency of an Incident is assessed by considering the number of users affected and the criticality of the system(s) affected, within the context of the reasons listed above. A HSSI is when the criticality and volume of users affected breaches pre-determined threshold levels defined within support schedules. For internally provisioned services (NHS Digital Service Provider), the NHS Digital are responsible for assigning the severity level. For services provisioned to the NHS Digital, the Service Providers are responsible for assigning the severity level and may consult with NHS Digital and or other Service Providers to help make this decision. However in cases of dispute the final decision on severity will be made by the NHS Digital Service Bridge / NHS Digital.

The decision to invoke the HSSI Management process must be made by the NHS Digital Service Bridge team member working at the time a call is received, or if out of hours this decision is the responsibility of the NHS Digital National Service Desk in the first instance or on call NHS Digital Service Management Escalation & Deployment Manager if the Incident has been escalated. The decision should be made after examining all information provided by either the NHS Digital for internally provisioned services or the Service Provider for externally provisioned services, but only when that Service Provider has confirmed the severity as 1 or 2 (unless overruling the internal and external NHS Digital Service Providers, see above).

Initial notification of a severity 1 or 2 Incident, will come from the internal and external NHS Digital Service Providers, Accredited Desk NHS Digital National Service Desk or where relevant, other Service Desks which support internal services. The NHS Digital Service Bridge will also pro-actively monitor the National Monitoring Service (NMS) tools currently available to the team during core hours. Based on the alerts generated from Events and Monitoring, the NHS Digital Service Bridge will take proactive action to alert internal and external NHS Digital Service Providers and instigate system health checks where potential problems may be occurring but will always confirm the situation with a internal and external NHS Digital Service Provider before communicating any HSSI. Additionally where information provided to the Service Bridge may indicate a potential problem (i.e. Incident logged as a Severity 3 or 4) action may be taken to investigate further with internal and external NHS Digital Service Providers to ensure prevention of a HSSI.

# Higher Severity Service Incident Management Process (Core hours)

A quick reference guide for NHS Digital internally provided services can be found in the [appendix](#_Appendix_I).

The following process diagram shows the high level steps to be followed, by the NHS Digital Service Management Service Bridge In Hours (08:00 – 17.30 Mon-Fri excluding bank holidays) from the point of receiving details of a severity 1 or 2 incident.

****

## Process Definition Details

| **Process Step** | **Owner** | **Definition** |
| --- | --- | --- |
| 1a. HSSI Reported | NHS Digital National Service Desk / Accredited Desk / Other internal Service Desk | The NHS Digital National Service Desk, Accredited Desk or other internal Service Desk receives details of an incident, following prioritisation, classification and triage the incident is assigned as severity 1 or 2. Incident details are recorded in the incident logging tool used by the NHS Digital National Service Desk or relevant Service Desk. |
| 1b. HSSI Reported | NHS Digital Service Bridge | The NHS Digital Service Bridge pro-actively identifies an issue or receives details of an incident, following prioritisation, classification and triage the incident is assigned an unconfirmed severity 1 or 2. Incident details are recorded in the incident logging tool used by the NHS Digital Service Bridge. |
| 1c. HSSI Reported | Service Provider | The Service Provider receives details of an incident, following prioritisation, classification and triage the incident is assigned as severity 1 or 2. Incident details are recorded in the incident logging tool used by the Service Provider. This includes NHS Digital support teams for internally provided services. |
| 2. Confirm HSSI with relevant supplier | NHS Digital National Service Desk | On an initial report of a HSSI from a user the NHS Digital National Service Desk must verify the severity with the relevant Service Provider. |
| 3. Provide confirmed HSSI details to Service Bridge | NHS Digital National Service Desk / Accredited Desk / Other internal Service Desk | The HSSI must only be reported to the NHS Digital Service Bridge once it has been confirmed by the supplier. |
| 4. Provide confirmed HSSI details to Service Bridge | Service Provider | The HSSI must only be reported to the NHS Digital Service Bridge once it has been confirmed by the supplier. The MDS in [**Appendix B**](#_Appendix_B) should be used by the Service Provider to give the minimum details. |
| 5. Initiate HSSI Procedures | NHS Digital Service Bridge | The NHS Digital Service Bridge records all information within the Incident Management Toolset |
| 6. Crisis Management Required | NHS Digital Service Bridge | The NHS Digital Service Bridge must assess if the HSSI fits the criteria to invoke Crisis Management Processes |
| 7. Security or Clinical Safety Risk | NHS Digital Service Bridge | The NHS Digital Service Bridge must assess if the HSSI fits the criteria to invoke Security or Clinical Safety processes. |
| 8. Security or Clinical Safety Risk | NHS Digital Service Bridge | The NHS Digital Service Bridge must flag the incident appropriately within the toolset and complete the additional Security or Clinical Safety minimum dataset fields and assign to the relevant team. |
| 9. Create Communications | NHS Digital Service Bridge | The NHS Digital Service Bridge will formulate SMS, Email and Service Status Web Page communications that are sent via a communications toolset to a list of pre-defined subscribers. Note that some Predefined Service are not communicated in this manner. Details of these services are stored locally on the Service Bridge. |
| 10/11. NHS Digital Incident diagnosis and Resolution | NHS Digital Service Bridge | The NHS Digital Service Bridge may call upon internal technical specialists to advise on incident resolution activity |
| 12. Drive Resolution | NHS Digital Service Bridge | The NHS Digital Service Bridge will update, escalate and drive resolution via war rooms as appropriate. |
| 13. Follow Internal Process | Service Provider | NHS Digital expects the supplier / internal support team to follow standard internal process for logging, classification, diagnostics and resolution of the incident. The supplier should provide updates to the Service Bridge throughout the lifecycle of the incident. |
| 14. Incident diagnosis Process | Service Provider | The Service Provider will follow internal processes for diagnosis and resolution of the incident. This will be done in conjunction with the NHS Digital Service Bridge Team through regular technical and management meetings/conference calls, led/facilitated by the NHS Digital Service Bridge |
| 15. Provide Regular updates of the incident until completion | Service Provider | NHS Digital expects the supplier to provide regular updates upon request with a guideline of every 90 minutes for a severity 2 HSSI and every 60 minutes for severity 1 HSSI. |
| 16. Provide Regular updates to the incident reporter | NHS Digital National Service Desk / Accredited Desk | The NHS Digital National Service Desk / Accredited Desk / other internal Service Desk should continue to update the end user with regards to progress of the incident reported, this can be achieved through relaying Service Bridge communications |
| 17.HSSI Resolution Activity | Service Provider | The Service Provider will follow internal processes for resolving HSSIs |
| 18.HSSI Resolved. | Service Provider | Through internal testing where applicable, the Service Provider will confirm if the HSSI is resolved |
| 19. Provide Full Resolution Details. | Service Provider | Provide full details of the resolution to the NHS Digital Service Bridge. Where a root cause is yet to be determined, a problem record number should be quoted. |
| 20.Send final HSSI communications | NHS Digital Service Bridge | A final service notification alert should be sent using the Communications Manager toolset. A summary of the resolution must be included. |
| 21. Close incident with resolution details. Update incident reporter | NHS Digital National Service Desk | The NHS Digital National Service Desk or other internal Service Desk will be notified of the resolution via the HSSI communications (Step 20). The NHS Digital National Service Desk or other internal Service Desk must confirm that the incident has been resolved directly with the end user before closure. |
| 22.HSSI Closed | NHS Digital Service Bridge | The NHS Digital Service Bridge resolves the incident record within the incident management toolset. |
| 23/24. Post Incident Review | NHS Digital Service Bridge | The NHS Digital Service Bridge is responsible for arranging & facilitating the Post Incident Review Meeting upon resolution of an incident. This will only be invoked at the discretion of the Service Bridge Manager and is not always required. |
| 25.Service Review | NHS Digital Service Bridge / Service Provider | The NHS Digital Service Bridge and the Service Provider is jointly responsible for ensuring a Service review Meeting is regularly arranged/attended with minutes and actions recorded and actioned. |

# Higher Severity Service Incident Management Process (Out of hours)

The following process diagram shows the high level steps to be followed, by the NHS Digital National Service Desk when acting as the Service Bridge out of hours (17.30 – 08.00 Mon-Fri and 17:30 Friday through to 08:00 Monday, including bank holidays) from the point of receiving details of a severity 1 or 2 incident.

## Process Definition Details

| **Process Step** | **Owner** | **Definition** |
| --- | --- | --- |
| 1. HSSI Reported | NHS Digital National Service Desk | The NHS Digital National Service Desk receives details of an incident that has been assigned a severity 1 or 2 severity level from the end user |
| 1a. HSSI Reported | Relevant Service Provider | The Service Provider receives details of an incident from NHS Digital National Service Desk, Accredited Desk, User-base or Monitoring. This includes NHS Digital support teams for internally provided services. |
| 2. Pre-assessment and Confirm HSSI | Relevant Service Provider | Following prioritisation, classification and triage the incident is assigned a severity 1 or 2 setting and notified to the NHS Digital National Service Desk on the Service Bridge number. |
| 3. Supplier confirmed | NHS Digital National Service Desk | The HSSI can only be progressed when this has been confirmed by the supplier. |
| 4. HSSI logged in SM Toolset | NHS Digital National Service Desk | The NHS Digital National Service Desk should log all HSSI details within SM Toolset. |
| 5. Has the supplier confirmed the HSSI? | NHS Digital National Service Desk | If the NHS Digital National Service Desk have not received confirmed acceptance of a HSSI within 20 minutes of initial notification to the supplier of a potential severity 1 or 2 HSSI, the supplier should be chased for confirmation. |
| 6. BAU HSSI? | NHS Digital National Service Desk | The NHS Digital National Service Desk must decide if the HSSI fits the HSSI NON BAU profile as detailed in [**Appendix G**](#_Appendix_G). If this is a BAU HSSI, proceed to step 11. If this is not then proceed to step 7. |
| 7.Contact Escalation & Deployment Manager | NHS Digital National Service Desk | Using the weekly distributed Escalation & Deployment Manager Rota, the NHS Digital National Service Desk will need to perform a look up to see which Escalation & Deployment Manager (EDM) is on call. Full details of the HSSI / query should be relayed over the telephone |
| 8.Incident handling advice and guidance | NHS Digital EDM | Based on the information provided by the NHS Digital National Service Desk. The NHS Digital EDM will provide guidance on how to onward manage the incident. |
| 9.Are HSSI comms required | NHS Digital EDM | NHS Digital EDM will advise if communications are required |
| 10.Communications handling advice and guidance | NHS Digital EDM | Based on the information provided by the NHS Digital National Service Desk. The NHS Digital EDM will provide guidance on what information to communicate if deemed necessary |
| 11. Send regular SMS & Email notifications to stakeholders. Regular checkpoint meetings. Update webpage | NHS Digital National Service Desk | If HSSI communications are required for the HSSI in hand, then the NHS Digital National Service Desk should use the standard template for creation of the communication, and follow the standard process for communicating this information out. This includes the Communications Manager and Service Status Page.  The Service Status webpage will updated automatically and throughout the lifecycle of the HSSI in line with the SMS and E-mail communications for services where they are required. |
| 12. Follow internal process | Relevant Service Provider | NHS Digital expects the supplier to follow standard internal process for diagnostics and resolution of the incident. The supplier should provide updates to the NHS Digital National Service Desk throughout the lifecycle of the incident as requested with general guidance of every 90 minutes for a severity 2 and every 60 minutes for severity 1 |
| 13. Incident diagnosis Process | Relevant Service Provider | The supplier will follow internal processes for diagnosis and resolution of the incident. This will be done in conjunction with the NHS Digital National Service Desk through regular technical and management telephone updates. |
| 14. HSSI resolution activity | Relevant Service Provider | The supplier will follow internal processes for resolution of the incident. This will be done in conjunction with the NHS Digital National Service Desk / EDM through regular technical and management telephone updates. |
| 15. Provide Regular updates of the incident until completion | Relevant Service Provider | NHS Digital expects the supplier to provide regular updates on the HSSI as defined in step 12. |
| 16. Escalation required | Relevant Service Provider  NHS Digital National Service Desk  NHS Digital EDM | An escalation regarding an ongoing HSSI can be initiated by either the Relevant Service Provider, NHS Digital National Service Desk, other internal Service Desk or NHS Digital EDM. All escalations should be raised to the NHS Digital National Service Desk and raised to the NHS Digital EDM. Advice and guidance will be issued to the NHS Digital National Service Desk. |
| 17. HSSI resolved? | Relevant Service Provider | Relevant supplier should perform checks to ensure the incident that is believed technically resolved is no longer being experienced by the end user. If yes, then Relevant ISP can progress to step 18. If No then the Relevant ISP should continue with step 13/14. |
| 18. Provide full resolution details – process to be followed to completion | Relevant Service Provider | Provide full details of the resolution to the NHS Digital National Service Desk. Continue to engage in the HSSIM Process until NHS Digital is satisfied. |
| 19. Send final comms. Update website. Update the HSSI Record. | NHS Digital National Service Desk | A final Service Notification Alert should be sent using the communications manager and the Service Status Page where required. The SM Toolset record closure details should be completed and set to a status of resolved. |

# HSSI Types

## Security Incidents

The Information Security Management - Incident Handling and Response Procedure provides a definition of an Incident, for the purposes of Security as:

*‘An incident is any unauthorised access, use, modification, or control of the Authority’s resources, any violation of the Authority’s security policies, or any attempt to defeat security mechanisms or exploit vulnerabilities and/or bugs which may exist within the Authority’s operational environment.’*

In the case of Security Incidents it may be necessary to modify the normal HSSI process. This is because security related Incidents may require specialist handling in order to manage possible press interest and/or management input regarding the resolution of the incident.

This section of the document defines what steps are to be taken in the event that a Security Incident, or possible Security Incident, comes to the attention of the NHS Digital Service Bridge.

A HSSI may result from a Security Incident, for instance if a service is taken down in order to limit possible damage from a Security Incident. Similarly an Incident may be the first sight that NHS Digital has of a possible Security Incident. It is therefore important that clear lines of communication exist between the NHS Digital Service Bridge, Information Security Team and Information Governance who have responsibility for data security.

Types of Security Incident include:

* Account compromise
* Behavioural vulnerability
* Corruption of Data / Information
* Denial of Service
* Disclosure (Misuse) of Data / Information
* Missing Patient Data
* Network compromise
* Password compromise
* Physical security
* Process vulnerability
* Root compromise
* Software vulnerability
* Theft – Data
* Theft – Physical
* Unauthorised Access and/or Use
* Virus

*This list is not exhaustive.*

## Security Incident Management

If notification of a Security Incident, or potential security, incident is received from a internal and external NHS Digital Service Provider, the NHS Digital National Service Desk, through proactive monitoring of incidents or through any other source, the NHS Digital Service Bridge or NHS Digital Escalation & Deployment Manager should immediately inform the NHS Digital Senior Management. The Service Bridge procedure for initiating a security risk assessment within the SM Toolset can be found in [Appendix A](#_Appendix_A).

The security flag should be ticked within the toolset incident record and a security record should be completed within the SM Toolset. The record will then be assigned via the toolset to the Security and I.G group**.** The incident assignment should be followed up with a phone call to ensure the incident has been received. Should security contacts be unavailable and the requirement for a security team contact is of an urgent nature then this should be escalated to a level 3 escalation point within NHS Digital.

As part of the role of the OST/IG contact in this process, it will be their responsibility to clearly identify any special requirements and to provide clear guidance of what, if any, communications are sent, which may include Press Office involvement if required *(*Press Office contact details can be found on theService Bridge Contacts Sheet. It will be the responsibility of the NHS Digital Service Bridge or NHS Digital Escalation & Deployment Manager to manage through to resolution any communications regarding the incident within the constraints of the IG requirements, but with the assistance of the IG Security Team where appropriate.

## Patient Identifiable Data (PID)

During investigations into Problems or Incidents it is sometimes required that a third party forwards information for use in, for example, the diagnosis of a live service Incident. However such information should not under any circumstances contain Patient Identifiable Data (PID) or any other data of a sensitive nature. Such data can be defined as information that allows the identification of an individual patient to be revealed, either explicitly or by implication.

It is the responsibility of all parties involved to ensure PID is not sent accidentally or handled incorrectly when it is sent. However Service Management team members must always:

1. Proactively check with a supplier that any data provided does not contain PID (or have any other security implications) prior to onward dissemination or that if it does then it is retransmitted via the correct means and only if essential.
2. Where possible a manual check will also be performed on data sent through before onward dissemination (although it is not always possible to read the information provided in the format it is in).
3. If PID is absolutely essential to facilitate investigation of an issue that it is provided in a way that upholds the Care Record Guarantee (e-Gif, encryption, known accesses etc.)

If for any reason a situation arises where a NHS Digital Service Management representative is unsure of how to proceed or is not 100% sure about what is being sent then it should be escalated to a senior manager immediately.

## Clinical Safety Incidents

Any HSSI that may have a clinical impact must be immediately reported to the Clinical Safety Team.

The clinical safety flag should be ticked within the SM Toolset incident record and the additional clinical minimum dataset (MDS) information should be completed. The incident will then be assigned via the toolset to the Clinical Safety Team**.** The incident assignment should be followed up with a phone call to ensure the incident has been received. The Service Bridge procedure for initiating a clinical risk assessment within the SM Toolset can be found in [Appendix A](#_Appendix_A).

The Clinical Safety Team will begin the process of defining if the HSSI is in fact a clinical safety issue or whether it is a standard HSSI. If it is defined as a clinical issue then from that point on the Clinical Safety Team takes full responsibility for the management of the clinical risk until it is deemed safe and the NHS Digital Service Bridge will maintain ownership of the incident record.

The Clinical Safety Team has the responsibility of interacting with the necessary clinical safety officers and clinicians both within NHS Digital and the internal and external NHS Digital Service Providers They will update the NHS Digital Service Bridge or NHS Digital Escalation & Deployment Manager where appropriate and let them know when support is required.

Out of hours the clinically impacting HSSIs will be escalated to the NHS Digital Escalation & Deployment Manager who should contact the Clinical Safety Team on call Safety Officer resource.

The NHS Digital Service Bridge and NHS Digital Escalation & Deployment Manager s have the responsibility to ensure all information that is available is provided within the incident record. The contact details for the Clinical Safety Team are in the NHS Digital Service Bridge Contact Sheet and on the NHS Digital Escalation & Deployment Manager rota.

Clinical Safety HSSI Incidents will be communicated out by the NHS Digital Service Bridge if there is any potential risk to patient care.

If a HSSI is raised and a patient(s) have already come to some harm then the NHS Digital Service Bridge will **NOT** communicate the incident.

# NHS Digital Service Bridge Key Inputs & Outputs



# Roles and Responsibilities

## NHS Digital Service Bridge (In Hours)

The objectives of the NHS Digital Service Bridge are to ensure internal and external NHS Digital Service Providers are operating in accordance with commercial and operational agreements agreed with NHS Digital, and to facilitate collaboration between resolver groups / stakeholders where no official relationships are agreed; to reduce the business impact and expedite the resolution of the HSSI.

Roles and Responsibilities:

* Provide dedicated major incident management telephone support.
* Ensure the required resources are being made available internally and by the Service Providers and that resolution plans are on track by regularly reviewing the HSSI with the Service Provider MIMs and internal technical teams.
* Escalate within internal and external NHS Digital Service Providers in a timely and constructive manner to break down any barriers to the resolution of the Incident.
* Schedule and agree the time of each checkpoint meeting/call. Internal and external NHS Digital Service Providers currently work to the guidance of updates to the NHS Digital Service Bridge every 60 minutes for a severity 1 and every 90 minutes for a severity 2 HSSI.
* If out-of-hours and where required, schedule and agree Emergency CAB Meetings.
* If the HSSI continues beyond the working day, a detailed handover must be provided to the NHS Digital National Service Desk in the format of an email template and telephone call.
* Facilitate cross supplier / internal support team war room activities to drive incident resolution.
* Facilitate checkpoint meetings where required.
* Arbitrate on HSSI severity disputes to ensure the correct severity is set by NHS Digital Service Providers.
* Manage Service Provider Higher Severity Incident Reports within 10 day policy.
* For NHS Digital internally delivered service HSSIs, on closure of an HSSI, the NHS Digital Service Bridge will ensure that the incident details are sufficient for a HSSIR to be generated.
* Issue regular communications to interested parties and ensure all communications are substantiated and based on the facts discussed and agreed during meetings or via any other communication channel.
* Perform end to end monitoring of fix time OLA’s (jeopardy management) for Incidents that have a severity 1 or 2 setting and will escalate to support teams where an Incident has reached its defined threshold or has breached its fix time OLA.
* Perform end to end monitoring of fix time OLA’s (jeopardy management) for High Priority Events that have a severity 1 or 2 setting and will escalate to support teams where an Event has reached its defined threshold or has breached its fix time OLA.
* Ensure the internal and external NHS Digital Service Providers conducts a Post Incident Review when required following an HSSI.

## NHS Digital National Service Desk (Acting as service Bridge Out of Hours)

Roles and Responsibilities

* For out of hours support: 17:30 - 08:00, Monday to Friday, weekends and bank holidays, the NHS Digital National Service Desk (acting as the Service Bridge) and a NHS Digital Escalation & Deployment Manager will be available. Please refer to the current NHS Digital Escalation & Deployment Manager rota which provides names and contact details for all of the NHS Digital Escalation & Deployment Managers. The weekly rota will be distributed each Monday morning by NHS Digital Service Management Team.
* NHS Digital National Service Desk must take on the responsibilities of the NHS Digital Service Bridge (With the exception of NMS monitoring).
* NHS Digital National Service Desk will only be responsible for the management of severity 1 or 2 HSSIs.
* NHS Digital National Service Desk must follow the same communications procedures as the NHS Digital Service Bridge.
* NHS Digital National Service Desk must provide a detailed handover to the NHS Digital Service Bridge at the end of the shift.

## Escalation & Deployment Manager

Roles and Responsibilities for the HSSI management process:

* The NHS Digital Escalation & Deployment Manager must be available as per the EDM Rota
* The NHS Digital Escalation & Deployment Manager will only be responsible for escalation and advice and guidance to the NHS Digital National Service Desk of severity 1 or 2 HSSIs.
* The NHS Digital Escalation & Deployment Manager will be responsible for escalating to Level 3 Management where required.
* The NHS Digital Escalation & Deployment Manager will host any multi-party conference calls which are required to progress HSSIs outside of core hours.

## NHS Digital National Service Desk, Accredited Service Desks and other internal Service Desks

The internal processes of the NHS Digital National Service Desk and other internal Service Desks in the capacity of Incident Management are out of scope for this document, however when any severity 1 or 2 Incident is identified, the NHS Digital National Service Desk or other internal Servie Desks are responsible for the following:

* For each Incident logged that initially assigned a severity 1 or 2 then this Incident must be logged with the relevant internal and external NHS Digital Service Providers for confirmation and investigation.
* The severity 1 or 2 Incident will only be reported to the NHS Digital Service Bridge once the relevant internal and external NHS Digital Service Provider has confirmed the severity. In the case of internally delivered NHS Digital services, The NHS Digital National Service Desk or other internal Service Desk will set the severity and assign accordingly.
* Provide hot handover (phone call) of HSSIs to both the NHS Digital Service Bridge and internal NHS Digital Service Providers.
* Update the Service Desk Parent Incident and all other associated Incidents as and when information becomes available from the internal and external NHS Digital Service Provider and NHS Digital Service Bridge.
* Provide communication updates on the HSSI to end users as appropriate.
* Once the HSSI has been resolved the Service Desk parent incident and all other associated Incidents should be updated with resolution details and closed.

## Service Provider Obligations

External Service Providers are responsible for the following:

* Severity 1 or 2 Incidents must be reported by phone to the NHS Digital Service Bridge within 20 minutes of Incident acceptance on 0300 303 4333.
* Suppliers must provide a minimum dataset of information to the NHS Digital Service Bridge on initial logging, update and closure. Full details of this MDS can be found within here **(**[**Appendix B**](#_Appendix_B)**).**
* Providing Higher Severity Incident Report within 10 working days of HSSI resolution **[(See Appendix F).](#_Appendix_F)**
* Provide an HSSI action plan upon reasonable request by the NHS Digital Service Bridge during an HSSI. Further details available within the HSSI Reporting section
* Ensure support to the NHS Digital Service Bridge and other suppliers during interoperable HSSI investigations.
* Provide responses and supporting data were required when NHS Digital monitoring events have been identified.
* Participate / provide feeds into State of the Nation Calls when required

## GPIT Service Provider Obligations

The Supplier is responsible for providing a technical fix to all HSSIs or significant HSSIs. The Supplier must work with the Service Bridge and other suppliers to support the resolution of the business impact of the HSSI or significant HSSI.  If any impact from the HSSI is propagated downstream to other systems, the Supplier must contact such downstream supplier and transfer ownership or work in partnership with that downstream supplier to resolve.

The Supplier must provide HSSI reports and undertake a post incident review of all HSSIs, if the root cause originated from the Supplier or one of its third party suppliers or Sub contractors. Those which have a clinical or IG impact or are sensitive in nature must be redacted by the Supplier prior to publication or sharing with the Service Bridge. The HSSI report must be shared with the Service Management Agent and Service Recipients within 5 Working Days [**(See Appendix F).**](#_Appendix_F) Where the root cause has not originated from the Supplier or one of its third party suppliers or Sub contractors, this should be reflected by the supplier on the HSSI Report title page. Once the root cause has been agreed with the Serivce Bridge onward publication of the HSSI will reflect this. The Supplier can either publish the HSSI Reports onto a portal accessible to all NHS stakeholders or provide the HSSI Reports to the Service Bridge to publish.

The Supplier must address any comments detailing a failure to meet the HSSI report quality criteria received from the Service Bridge on HSSI reports and must re-submit the HSSI report for further Service Management Agent review within 24 hours of feedback receipt. This process must continue until the Service Bridge accepts the HSSI report.

## NHS Digital Internal Support Teams / Resolver Groups

Internal NHS Digital Service Providers are responsible for the following:

* When severity 1 or 2 incidents are received into incident queues, they must be assessed immediately by the support area.
* Support areas must provide regular updates to the incident record at a minimum frequency of every 60 minutes for a severity 1 and every 90 minutes for a severity 2. This should be followed with a phone call to the Service Bridge to relay the incident update.
* Provide an HSSI action plan upon reasonable request by the NHS Digital Service Bridge during an HSSI. Further details available within the HSSI Reporting section.
* Ensure support to the NHS Digital Service Bridge and other suppliers during interoperable HSSI investigations.
* Provide responses and supporting data were required when NHS Digital monitoring events have been identified.
* Participate / provide feeds into State of the Nation Calls when required.

# State of the Nation Process

Where HSSI resolution or workaround activity has been undertaken by a internal and external NHS Digital Service Provider, an immediate ring around of an agreed set of critical users / Service Providers for the services impacted will sometimes be required to assure activity as quickly as possible. This process is known as the State of the Nation Process.

A group of contacts has been defined and agreed to provide relevant information from their organisation or from further contacts they have in end user care settings. These contacts cover users of services including but not limited to Spine Core, Care Identidy Service (CIS), the NHS e-Referral Service and GP2GP across various care settings.

When this requirement occurs the process is for one or more members of the NHS Digital Service Bridge to contact a sample stakeholder organisations for them to give current user impact analysis. Example organisations are detailed below:

* EMIS – Primary Care supplier covering NHS e-Referral Service, Spine Core, CIS & GP2GP.
* Vision – Primary Care supplier covering NHS e-Referral Service, Spine Core, CIS & GP2GP.
* DXC – Secondary Care supplier covering NHS e-Referral Service, Spine Core & CIS.
* Telephone Appointment Line – NHS e-Referral Service.
* Lloyds Pharmacy – EPS prescriber covering Spine Core.

In addition to these contacts the NHS Digital Business Relationship Managers within the Implementation and Business change profession may be engaged who have representatives that will engage with end users in Acute and Primary Care Trusts to gauge end user impact.

This process only operates during the normal business day as most of the contacts are only available during those times.

# Communication

It is the responsibility of the NHS Digital Service Bridge, or the NHS Digital National Service Desk out of hours, to produce and distribute any communications or Service Notification Alerts as required.

As a general rule all HSSIs should be communicated out using a Service Notification Alert, however there are exceptions to this such as when a HSSI is reported initially as resolved or when there is a clinical or security Incident. In these instances the Service Bridge will make a decision whether to communicate a HSSI on a case by case basis. Guidance on communicating retrospective HSSIs can be found later in this section. There are three key media used for communicating HSSIs, these are SMS, email and web.

When communicating out to the wider NHS, a consistent approach should be adopted in order that an audit trail of updates can be established*.* To assist in this process the Service Bridge Communications Manager (<http://servicebridge>) is required to be used, this broadcasts the notifications using all 3 media types listed above, with the web updates automatically updating on the NHS Digital Service Status Page. It is also essential that communications are released in a timely manner, ensuring that all stakeholders of the HSSI are kept up to date on the progress. Below is a guide to when communications should be made although ultimately it is down to the discretion of the individual dealing with the HSSI:

**First Service Notification Alert** – New HSSI – Using the Service Bridge Communications Manager, this should be made within 20 minutes of the confirmed HSSI being reported by the internal or external NHS Digital Service Providers. It should contain the initial information on the HSSI, it’s user impact, location (including NHS Trust / CCG) and Incident reference number, as well as stating the time of the next update. General guidance is every 1 hour for a severity 1 Incident and every 1.5hrs for a severity 2 Incident).

**Subsequent Service Notification Alerts** – Subsequent communications should be issued using the Service Bridge Communications Manager every hour for Severity 1s and every hour and a half for Severity 2 HSSIs. These updates should contain ongoing information on the Incident from the internal / external NHS Digital Service Providers as well as stating the time of the next update. These update times may vary at the discretion of the NHS Digital Service Bridge. This may apply in cases where the internal / external NHS Digital Service Providers are unable to provide an update, where waiting on parts delivery, code fixes or have been unable to contact end users after making reasonable attempts to do so.

**Final Service Notification** **Alert** – HSSI Resolved – This should be issued as soon as the internal / external NHS Digital Service Provider has confirmed the HSSI resolved irrespective of when the next update was due and must give summary details of the resolution. Once again, this needs to be issued using the Communications Manager.

**Retrospective HSSIs -** HSSIs Reported as Already Resolved

There are occasions when a internal / external NHS Digital Service Providers will report an HSSI to the NHS Digital Service Bridge or NHS Digital National Service Desk that has already been resolved. A decision point process has been put in place:

***NHS Digital Service Bridge would automatically send retrospective communications for all HSSIs if the HSSI is notified to the Bridge within 60 minutes of HSSI resolution. If the HSSI is notified outside of 60 minutes of resolution then the NHS Digital Service Bridge would request confirmation from the relevant Service Owner on whether retrospective communications should be sent or through Service Owner leads if the Service Owner is not available.***

This is to ensure that the already resolved HSSIs don’t detract from the importance of open HSSIs but visibility of the HSSI is maintained.

## Programme Director Communications

In addition to the standard communications, there is a requirement to communicate select HSSI information to NHS Digital Directors and Group Programme Directors. To facilitate communication at this level, two distribution lists have been set up within the communications manager toolset. The following criteria for use have been specified below, against each distribution list:

**List 1. Programme Director List**

Datacentre HSSI- Any Type of Incident

Multi Site HSSI - Any Type of Incident

Key Deployment Site HSSI (currently any Lorenzo) - Outage Only

National Service HSSI - Performance Incident or Outage

Clinical Safety HSSI - Significant Risk to Patient Care

IG & Security HSSI - Significant risk to Confidentiality, Integrity or Availability

**List 2. Director List Top Level**

Datacentre HSSI - Outage Only

Multi Site HSSI - Outage Only

Key Deployment Site HSSI (currently Lorenzo) - Outage Only

National Service HSSI - Outage Only

Clinical Safety HSSI - Significant Risk to Patient Care

IG & Security HSSI - Significant risk to Confidentiality, Integrity or Availability

The above lists are to be used to conjunction with the existing communication policy and they are to be issued 24x7 by the NHS Digital Service Bridge or NHS Digital National Service Desk. Due to an element of subjectivity around the decision to issue the communication to either group, please refer to the internal procedure document named 'Director Level Communication Guide' forfurther advice and guidance.

## Management Only Communications

The NHS Digital Service Bridge will receive notifications from internal and external NHS Digital Service Providers as well as event management feeds when a non-service impacting national Incident has occurred, examples of this would be loss of resilience at a key data centre, or core messaging suspensions. Due to the non-service impacting nature, standard HSSI communications will not be sent, however key internal stakeholders will need to be informed. Within the Service Bridge Communications Manager toolset, the NHS Digital Service Bridge maintains a management only SMS and email distribution list.

During core hours the NHS Digital Service Bridge are responsible for making decisions on the suitable use of this communication channel. Outside core hours the NHS Digital National Service Desk will seek guidance from the NHS Digital Escalation & Deployment Manager.

## Early Life Support Communications

Following the role out of a new NHS Digital managed service or substantial upgrade it may be necessary to set up a restricted communications list during early life support. Requirements for closed group communications would be defined by the NHS Digital Service Owner who would agree the list at the point of scoping the Deployment Verification Criteria (DVC), in conjunction with the relevant programme or business unit. Where a closed group communications list has been defined, normal BAU open communications will resume from the point of full roll out approval (FRA).

# Escalation

There is an escalation process in place within the NHS Digital Service Management Team to ensure that any HSSI which requires additional senior management support, (e.g. as a result of a transition) and where applicable re-prioritisation of other work, will be available at any time it is required (24\*7). In addition to bringing senior level attention to the incident, this will also help reduce the risk of the HSSI being stalled and subsequently will mitigate the risks of further increasing the impact of the Incident.

Escalation of an HSSI should be carried out at the discretion of the NHS Digital Service Bridge or on call NHS Digital Escalation & Deployment Manager. The escalation points of contact are detailed in the weekly NHS Digital Escalation rota. There are guidelines for determining when to escalate detailed in [**Appendix C**](#_Appendix_C)**.**

# End Point Disablement

In the event that a system or service is significantly impacting, or has the potential to impact, the availability or integrity of NHS Digital systems or services, the disablement of an endpoint or a group of endpoints will be invoked. In this event, a 'war room' will be set up by the Service Bridge and the following stakeholders, when appropriate to their area of accountability, invited to review the risks and issues:

* Head of Service Management
* Service Management Lead / Senior Service Manager for Service Operations & Transition
* Relevant Service Owner
* Relevant Programme Representative
* Relevant Technical Representative
* Clinical Safety Representative
* Security Representative

Outside of core hours the NHS Digital Escalation & Deployment Manager will set the ‘war room’ up with the relevent stakeholders from the above list where available and include the level 3 Escalation Manager.

Following review, a level 3 decision will determine if the disablement of endpoint(s) is the appropriate course of action. On agreement of this action, a change request will be raised by the NHS Digital Service Bridge for implementation by the NHS Digital Technical Solutions Team (Service Management DIR Team) to disable the end point(s).

A management summary document will be drafted by the NHS Digital Service Bridge to advise senior management of the action taken. A letter will drafted by the relevant Service Owner to advise the Service Provider of the impacted systems or services of the action taken and the steps necessary to allow re-enablement. The re-enablement of the end point(s) would be managed through SCN/RFC for CAP introduced suppliers and by RFC for National suppliers.

**Examples of potential scenarios:**

* Misbehaviour of a site/product by sending misinformation or malformed messages to the Spine which could have a detrimental effect on patients, other services or Spine itself.
* Misbehaviour of a site/product sending a high number of requests to Spine which exceeds expected volumes and has the potential to cause degradation of service to the Spine user base.

In situations where a supplier system is causing these issues to occur, wherever possible NHS Digital will work with the supplier to explore any other avenues of activity which could be taken to mitigate the issues prior to disabling the endpoint.

# Change Management

An emergency change should only be presented to NHS Digital to resolve or to prevent an HSSI. This section describes the interactions between the Change and Higher Severity Service Incident Management processes, highlighting differences in responsibilities depending on the timing of the situation.

* The Change Management Team operates between 09:00 - 17:00, Monday to Friday. During these times all changes, including Emergency changes will be dealt with by the Change Management Team as per business as usual processes. *This document does not describe the BAU change process.*
* The NHS Digital Escalation & Deployment Manager and or Core Service Bridge Team will take responsibility for any changes deemed ’Emergency’ in the periods 17:00 - 09:00 Mon-Fri, as well as Saturdays, Sundays and bank holidays

The Service Management NHS Digital Escalation & Deployment Manager is responsible for organising, facilitating and recording the Emergency CAB.

In the absence of a documented RFC, the supplier / internal support team MUST be able to verbally advise on the following aspects of the change:

* + Summary of the proposed change and the environment(s) affected;
  + Planned time of implementation (both start and finish);
  + Summary of the impact of the change, including details of any associated risks and how they will be mitigated;
  + Details of any impact on or engagement needed by other suppliers as a result of the proposed change;
  + Clear rationale on why this must be implemented out of hours versus being done via BAU processes;
  + Details of the success criteria relating to the change;
  + Details of any pre-implementation and post implementation tests which the supplier will undertake to minimise further threats to service and ensure the validity of the change;
  + Details of how the change will be implemented;
  + Details of how the change will be backed out if there are any problems.
* The facilitator of the Emergency CAB Meeting must record the outcome of the meeting. If an RFC is rejected, clear and documented details on the reason for the decision should be included. Both rejections and approvals should be sent immediately after the Emergency CAB and sent to both the Supplier Major Incident Manager / Internal support team and NHS Digital Change Management [changemgmt@nhs.net](mailto:changemgmt@nhs.net)
* The Service Management NHS Digital Escalation & Deployment Manager acts as the decision point for approval or rejection of the Emergency RFC, if there is any doubt as to validity of the request, the NHS Digital Escalation & Deployment Manager should either reject the change or seek advice/clarification from one of the designated NHS Digital Service Support escalation points
* The Service Provider / internal support team must undertake to provide updates on the progress of the change to the Service Management NHS Digital Escalation & Deployment Manager and should advise when the change is fully complete (or backed out).
* Where any pertinent information or activity has occurred an appropriate hand-over should be made to Change Management and the NHS Digital National Service Desk or NHS Digital Service Bridge as per BAU handover procedures.

Full details of the Emergency Change Process / terms of reference is detailed within[**Appendix D**](#_Appendix_D).

# NHS Digital Service Management Handovers

## Service Bridge

At 17:30 Monday to Friday a member of the NHS Digital Service Bridge team should ensure that the NHS Digital National Service Desk analysts taking over are verbally informed of any HSSIs that have occurred and if any out of hour's activity is expected. This should always be followed up with a documented handover confirming the details of any ongoing HSSIs as per the Service Bridge Handover Template. If no HSSIs have occurred, a telephone handover is still required to the NHS Digital National Service Desk informing them that no HSSIs are currently running. This also assures that the telephone divert has been successfully set up.

## NHS Digital National Service Desk

The NHS Digital National Service Desk should provide a detailed update to the NHS Digital Service Bridge at the end of the shift. All new HSSIs and updates on existing HSSI should be detailed on the SM Toolset. Information on any other issues should also be provided verbally during the handover including any management only information messages sent during the shift. This should always be followed up with a documented handover confirming the details of any ongoing HSSIs as per the NHS Digital National Service Desk Handover Template.

The NHS Digital National Service Desk are also responsible for updating the incident record with information provided by the NHS Digital on call Escalation & Deployment Manager to facilitate a complete handover back to the NHS Digital Service Bridge

If there is nothing to report then a call should be placed to the NHS Digital Service Bridge to say there is no handover as this assures that the telephone divert has been successfully removed by the NHS Digital Service Bridge.

## NHS Digital Escalation & Deployment Manager

The NHS Digital Escalation & Deployment Manager should ensure that the NHS Digital National Service Desk is fully informed of all escalation information and issues pertaining to any HSSIs currently being managed. If an incident requires the ongoing involvement of a NHS Digital Escalation & Deployment Manager such as over a weekend shift, then the NHS Digital Escalation & Deployment Manager should provide both verbal and written handover information to the next on shift NHS Digital Escalation & Deployment Manager. Further details of this process can be found within the Escalation & Transition Manager Guidelines in [**Appendix E**](#_Appendix_E).

# HSSI Reporting

The Higher Severity Service Incident Review Process should commence as soon as the HSSI is resolved. Suppliers are required to provide a Higher Severity Service Incident Report (HSSIR) for every managed HSSI. On occasion where an incident has an associated high profile, NHS Digital may also request the drafting of a Management summary report. For internal NHS Digital Services these are produced by the Service Bridge with input from the relevant internal resolver groups.

## Higher Severity Service Incident Report

Higher Severity Service Incident Reports (HSSIR’s) are produced by each NHS Digital Service Provider to provide a summary of the Higher Severity Service Incidents that have taken place. The report details key incident information including resolution steps taken and any root cause information known at the point of writing the report. The report is due to be provided to the NHS Digital Service Bridge by each NHS Digital Service Provider no more than 10 working days after closure of the incident. A template detailing the level of information required is available within [**Appendix F**](#_Appendix_F)**.**

The report provides a key link between the NHS Digital Service Bridge and the problem management process along with giving the users the ability to understand key information surrounding an incident. Following NHS Digital Service Bridge Review and the removal of any sensitive information, the report is available to relevant stakeholders affected by the HSSI upon request.

For NHS Digital internally delivered service HSSIs, on closure of an HSSI, it is the responsibility of the NHS Digital Service Bridge to ensure that the incident details are sufficient for a HSSIR to be generated.

## HSSI Action Plan

An HSSI action plan may be requested at the discretion of the NHS Digital Service Bridge or NHS Digital Service Owner during an HSSI. This is more commonly requested during long running and complex HSSIs and is required to give assurance to NHS Digital that the internal and external NHS Digital Service Provider and relevant resolver group are following a systematic resolution approach. The action plan is expected to be a living document for the duration of the HSSI and will often be used to steer war room investigations. Whilst there is no set format for this, it is expected that an action plan will detail the following points:

* Investigations to date
* Identified clinical or security risk and any mitigations put in place / required
* Breakdown of proposed resolution activity split into logical work streams
* Expected timescales for competition of each resolution / work stream activity

## Management Summary Report

A management summary report can be requested both during and after an HSSI where an HSSI has senior management interest and a higher level of information is required. This will only be requested when absolutely required and will be formerly requested verbally by the NHS Digital Service Bridge. Specifics of what is required will be detailed at the time of request. As a minimum, the following level of detail would be required:

* Date/time of occurrence of the HSSI
* Date/time of resolution of the HSSI if resolved
* Impact – Business / Financial / Clinical / Security
* Activity to date
* Summarised explanation of resolution work around implemented if known
* Summarised explanation of the cause if known
* Planned Activity / Action Plan

# Post Incident Review

The NHS Digital Service Bridge is responsible for arranging & facilitating a Post Incident Review meeting upon resolution of a HSSI. This will only be invoked at the discretion of the HSSI Service Bridge in conjunction with the relevant Service Owner and is not always required. Involvement in this meeting will come from appropriate members of the resolving team, plus other technical representatives that may be allocated actions, e.g. design authority or application development. The Problem Management function within Service Management Cells should also attend to establish any links between these observations and any existing issues on the known problem registers and to take responsibility of any Problems created as a result of the HSSI.

The purpose of the Post Incident Review meeting is to review:

* What caused the incident?
* How efficiently it was resolved?
* Can it be prevented from occurring again?
* Could this incident have been prevented?
  + How?
* Could it have been diagnosed faster?
  + How? What Tools? Additional skills? Etc.
* Any issues encountered?
* Lessons learned?
* Any actions arising to address any of the above.

Actions and Lessons Learned output from PIRs will be tracked and maintained on the Service Bridge PIR tracker which is accessed via the Service Bridge Confluence Page.

# Appendix

The following documents provide additional reference points and guidance in relation to the NHS Digital HSSI process.

## Appendix A

Service Bridge Clinical Safety and Security Incident Management Procedure (embedded doc checked on: 20/07/2020)



For the latest version of the embedded document please click [here](https://hscic365.sharepoint.com/sites/SMHUB/Guidance%20Library/Clinical%20Safety%20and%20Security%20Incident%20Management%20Procedure.docx).

## Appendix B

HSSI Logging MDS (embedded doc checked on: 20/07/2020)



For the latest version of the embedded document please click [here](https://hscic365.sharepoint.com/sites/SMHUB/Guidance%20Library/HSSI%20Minimum%20Data%20Set%20and%20Information%20Flow%20Guidance.docx).

## Appendix C

Escalation Guidelines (embedded doc checked on : 20/07/2020)



For the latest version of the embedded document please click [here](http://teams2/sites/SMHUB/Guidance%20Library/HSSI%20Escalation%20Guidelines.docx).

## Appendix D

Emergency Change Advisory Board (CAB) Terms of Reference (embedded doc checked on : 20/07/2020)



For the latest version of the embedded document please click [here](https://hscic365.sharepoint.com/sites/SMHUB/Guidance%20Library/NHS%20Digital%20SM%20National%20Change%20Management%20CAB%20TOR.docx).

SM National Change Management Policy (embedded doc checked on : 20/07/2020)



For the latest version of the embedded document please click [here](https://confluence.digital.nhs.uk/display/SM/Central+Change+and+Configuration+Management+Team).

## Appendix E

Escalation & Transition Manager Guidelines (embedded doc checked on : 20/07/2020)

****

For the latest version of the embedded document please click [here](https://hscic365.sharepoint.com/sites/SMHUB/Guidance%20Library/NHS%20Digital%20Escalation%20and%20%20Deployment%20Managers%20Guidance.docx).

## Appendix F

Higher Severity Service Incident Report Template (embedded doc checked on: 20/07/2020)



For the latest version of the embedded document please click [here](http://teams2/sites/SMHUB/Guidance%20Library/NHS%20Digital%20HSSI%20Report%20Template.docx).

## Appendix G

Supplier Scorecard Criteria

The central supplier scorecard for supplier interaction with the Service Bridge has redacted and targets will be set up with suppliers on an individual basis.

## Appendix H

NHS Digital Severity Level Guidelines (embedded doc checked on: 20/07/2020)

****

For the latest version of the embedded document please click [here](http://teams2/sites/SMHUB/Guidance%20Library/NHS%20Digital%20-%20Severity%20Level%20Guidelines.docx).

## Appendix I

NHS Digital HSSI Quick Reference Guide for NHS Digital Internally Provided Services (embedded doc checked on: 20/07/2020)

****

For the latest version of the embedded document please click [here](https://hscic365.sharepoint.com/sites/SMHUB/Guidance%20Library/HSSI%20Quick%20Reference%20Guide.docx).