Meeting of BNSSG ICB Board

Date: Thursday 5th September 2024
Time: 15:30 – 17:00
Location: Bristol Citadel Community Church and Family Centre, 6 Ashley Road, St Paul's, Bristol BS6 5NL

Agenda Number:	6.2	
Title:	**Digital Incident Management Process**	
Confidential Papers	**Commercially Sensitive**	No
	Legally Sensitive	No
	Contains Patient Identifiable data	No
	Financially Sensitive	No
	Time Sensitive – not for public release at this time	No
	Other (Please state)	No
Purpose: Decision		
Key Points for Discussion:		

Our Digital Vision has a clear commitment for us to *become an exemplar of a digitally advanced ICS.* A robust Digital Business Continuity Plan (DBCP) is an essential foundation for achieving this vision.

We have recently experienced several significant IT outages that have caused operational issues across our system. These were global outages beyond our local control but this has prompted an urgent revision of our digital continuity plans to incorporate lessons learned.

As a Board it is critical that we are assured that we have high quality processes and well maintained documented procedures that guides our organisation and the wider system to respond, recover, resume and restore to a pre-defined level of operation following disruption. (As referenced in ISO22301:2019) This plan is focused specifically on the digital components of our system recovery.

This document forms part of the wider ICB Business Continuity Plan and outlines

1. the system wide principles and framework for Digital Incident Management
2. how the ICB intends to respond to any digital incidents impacting its core digital applications
3. the role of the ICB in supporting its ICS partners in executing their Business Continuity Plans

Recommendations:	• To discuss and approve the Digital business continuity plan • To outline any specific areas of Board interest / education and reporting that may be required
Previously Considered By and feedback :	• System Bus continuity Teams • Crowdstrike Incident Team • ICB EPRR Team • Strategic Informatics Group
Management of Declared Interest:	None
Risk and Assurance:	Addresses the following risks • ICB Cyber Security Risks • Provides mitigation and support to all aspects of business continuity risks held across the system. • All risks linked to different components of digital services failures or outages
Financial / Resource Implications:	There is no specific financial impact of the revision to this process
Legal, Policy and Regulatory Requirements:	This process supports our alignment with the following legal and statutory requirements Civil Contingencies Act 2004 Health and Social Care Act 2012 ISO22301:2019 NHS England Business Continuity Toolkit 2023
How does this reduce Health Inequalities:	The purpose of this process to consider how we try to mitigate a reduction in access of services to our population, when responding to an incident. As we develop each of the Digital handbooks a key section in the contingency plan will reflect any aspects of contingency actions that will need to reflect particular groups within our population
How does this impact on Equality & diversity	As we develop each of the Digital handbooks a key section in the contingency plan design will reflect specific needs. For example we will ensure that the policy has a screen readable version
Patient and Public Involvement:	N/A
Communications and Engagement:	Once this has been agreed we will communicate through EPRR routes and through Digital Leaders
Author(s):	Andy Carpenter: ICB Digital Lead
Sponsoring Director / Clinical Lead / Lay Member:	Deborah El-Sayed, Chief Transformation and Digital Officer

Digital Incident Management Process

Bristol, North Somerset & South Gloucestershire Integrated Care Board

Table of Contents

Introduction

The Bristol, North Somerset & South Gloucestershire Integrated Care Board (BNSSG ICB) Digital Vision is '*to become an exemplar of a digitally advanced ICS'.*

This will be achieved by working collaboratively and optimising design, data and modern technology to make ground-breaking improvements for the health and well-being of our population.

The six aspects of the Vision are:

- The benefits and opportunities of digital and data are embedded in our integrated design process
- We have a robust collaborative digital infrastructure that allows frictionless working for our staff across the full range of care settings
- We avoid duplication by integrating and reusing systems, architecture, shared services, support and expertise
- The experience of integrated seamless care for the person is underpinned and enabled by digital functionality and infrastructure that supports staff working
- Digital first channels are available for our citizens, empowering them to self-serve and make choices about their care journey
- Our integrated data-sharing and planning platform helps us to make the right decisions for people and our system

Without a robust Business Continuity Plan we cannot achieve our Vision. Improving our digital infrastructure and security, through single sign-on and common cyber standards, and providing seamless and timely information sharing between all health and care providers form core part of our digital transformation priorities.

A Business Continuity Plan is defined as a documented procedure that guides the organisation to respond, recover, resume and restore to a pre-defined level of operation following disruption. (ISO22301:2019)

This Incident Management Process document forms part of the ICB Business Continuity Plan and outlines:

1. The system wide principles and framework for Digital Incident Management
2. How the ICB plans to respond to any digital incidents impacting its core digital applications
3. The role of the ICB in supporting its ICS partners in executing their Business Continuity Plans

Digital Incident Management

Digital Incident Management is a structured process that organisations use to respond to and manage the aftermath of digital disruptions or security breaches. In today's hyper-connected world, businesses and institutions increasingly rely on digital infrastructure to operate efficiently. However, with this dependence comes the inevitable risk of digital incidents—unplanned events such as cyberattacks, system failures, data breaches, or software vulnerabilities that can severely impact business operations.

Effective digital incident management involves the identification, assessment, and resolution of these incidents to minimise damage and restore normal operations as swiftly as possible. It is not just a reactive measure but also a proactive approach that includes planning, monitoring, and continuous improvement to prevent future incidents.

The process typically involves a well co-ordinated effort across various teams, including IT, security, and compliance, to ensure that all aspects of an incident are managed efficiently. With the increasing complexity of digital ecosystems, a robust incident management strategy is essential for mitigating risks, protecting sensitive data, and maintaining business continuity in the face of potential digital threats.

The BNSSG ICB is responsible for ensuring business continuity management, including the development and maintenance of Business Continuity Plans (BCP), for the critical activities within their area of responsibility and this includes assurance from external service providers. It is important that all staff are aware of the BCP and the effects it will have on their areas of work.

Purpose

The purpose of a Digital Incident Management Process document is to provide a clear and comprehensive framework for effectively managing digital incidents within the BNSSG ICB. This document outlines the procedures, roles, and responsibilities necessary to identify, respond to, and recover from incidents that could disrupt digital operations. By defining a structured approach, it ensures that all team members are aligned in their actions, minimising the impact of incidents and facilitating a swift return to normal operations. Additionally, it serves as a reference to continuously improve the organisation's preparedness and resilience against future digital threats. Incident Management is the process responsible for managing the lifecycle of all incidents in line with ITIL[1] framework.

Scope

The following digital services are in scope of this Incident Management Process:

- ICB Corporate Services
- Connecting Care (Shared Care Record)

[1] ITIL: The Information Technology Infrastructure Library (ITIL) is **a set of practices and a framework for IT activities such** as IT **service management (ITSM) and** IT **asset management (ITAM)** that focus on aligning IT services with the needs of the business

- Primary Care Digital Services
- The process of managing ICS-wide digital incidents

This document does not cover the response to digital incidents in each of the ICS partner organisations except when these directly impact services provided by other ICS partners and where ICS wide response and execution of Business Continuity Plans is required.

The South, Central and West Commissioning Support Unit (CSU) are the main provider of digital support services to the ICB and therefore this document is developed to ensure alignment with their DDaT Incident Management Policy. (Appendix A)

How this document is structured

This document is structured as follows:

- Section 1: Definition of each incident type
- Section 2: Handbook for each core service:
    - ICB Corporate Systems
    - Connecting Care – Our Shared Care Record
    - Primary Care Systems
    - ICS Wide Major Incident

Each of the Section 2 handbooks contain

- A brief description of the services in scope
- The process to follow in response to the incident, depending on the incident type
- Key contact details – both during normal working hours and out-of-hours
- The timescales that we work to resolve the incident
- Suggested actions to ensure continuity of services

Section 1- What defines an Incident

A digital incident is an event or occurrence that disrupts or threatens to disrupt an organisation's digital operations, systems, or data. These incidents can range from cyberattacks, such as malware infections, ransomware, and phishing, to technical failures, like system crashes, software bugs, or network outages. Digital incidents can also include unauthorised access to sensitive data, data breaches, or insider threats. The impact of a digital incident can vary from minor inconveniences to severe consequences, such as data loss, financial loss, reputational damage, or legal ramifications. Properly managing digital incidents is crucial for minimising their impact and ensuring the continuity and security of an organisation's digital environment.

The BNSSG ICB defines digital incidents within the following groups:

Standard Incidents

A standard incident refers to a routine or relatively minor issue that occurs within an organisation's operations, typically handled through established procedures without the need for significant escalation. These incidents are common and usually have a well-defined resolution process, requiring minimal time and resources to address. Examples of standard incidents include minor technical glitches, password reset requests, or a temporary slowdown of a system. Unlike critical or major incidents, standard incidents do not pose a significant threat to the organisation's operations, security, or data, and their impact is generally limited and quickly resolved.

Example of a standard incident

A user reports a faulty printer in a GP consulting room, but since there are alternative printers available in other consulting rooms, the initial high impact and urgency of the situation are reduced.

P1 Incidents

A P1 (Priority 1) incident is the most severe level of incident in an organisation's incident management framework. It represents a critical issue that causes a major disruption to essential business operations or services, often impacting multiple users or systems. A P1 incident typically requires immediate attention and swift resolution due to its potential to significantly affect the organisation's productivity, revenue, or reputation.

Examples of P1 incidents might include a complete network outage, a critical system failure, a widespread security breach, or any event that causes significant operational downtime. The response to a P1 incident usually involves a coordinated effort from multiple teams, including IT, security, and management, to resolve the issue as quickly as possible and minimise the impact on the organisation.

Example of P1 incident

An entire GP site with loss of access to the network; unable to access any network related application including network drives, internet, email, or clinical system with no alternative workaround in place.

Major Incidents

A major incident is a serious event that causes a significant disruption to an organisation's critical operations or services, often requiring immediate and coordinated action to resolve. Unlike standard incidents, a major incident typically affects a large number of users, systems, or business processes, and has the potential to result in considerable financial loss, reputational damage, or regulatory consequences.

Major incidents are characterised by their high impact and urgency, often involving critical systems or infrastructure failures, widespread service outages, or severe security breaches. The response to a major incident usually involves mobilising a cross-functional incident response team, including IT, security, communications, and leadership, to manage the situation, communicate with stakeholders, and restore normal operations as quickly as possible. The process also typically includes thorough documentation and a post-incident review to identify the root cause and implement measures to prevent future occurrences.

Example 1

Multiple sites across the ICB with total loss of network connection and prolonged outage. All sites unable to access any network related application including network drives, internet, email or clinical system with no alternative workaround in place.

Example 2

Multiple sites across the ICB experiencing a cyber-attack preventing ability to access data from servers and across the network.

Service Level Agreement

A **Service Level Agreement (SLA)** is a formal, documented agreement between a service provider and a client which defines the level of service expected from the service provider. It outlines the specifics of the service being provided, including performance metrics, responsibilities, and expectations. They are used to ensure that all parties have a clear understanding of the service standards. SLAs are crucial for managing expectations, ensuring accountability, and providing a clear framework for resolving disputes between service providers and clients. There are SLA's within each service, details of which are available within the EPRR team. Specific SLA's will be available within internal documentation.

Below is **an example** of an SLA for digital services.

	Minimum	Standard	High Availability
	If default cannot be applied (justification)	*Default Level*	*24/7 service*
Support Hours	08:00 – 18:00	07:00-19:00	00:00-24:00
Hours Per Day	10	12	24
Supported Days	MTWTF	MTWTF	MTWTFSS
Bank Holiday	No	No	Yes
Availability Targets	98.5%	99%	99.9%

Example SLA

Digital Incident Management Process

The objectives of the Digital Incident Management Process are to ensure that standardised procedures are followed for efficient response, analysis, documentation, ongoing management and reporting of incidents. It supports clear visibility and communication and alignment with the wider business processes and protocols for incident management and business continuity.

This process is relevant to all digital incidents and should be followed regardless of the system or services impacted.

• Incident Identification

- **Detection**: Incidents can be identified through various means, including users, automated monitoring systems, user reports or routine checks.
- **Incident Logging:** Inform the South, Central and West CSU Helpdesk of the issue. They will record the incident and complete an initial assessment. Effective identification and logging of incidents are crucial for managing and mitigating their impact, ensuring a swift response, and improving future incident management practices.
- **Incident Prioritisation:** The CSU Team will prioritise the incident depending in its severity and impact to services and assign an Incident Manager.
- **Initial Assessment**: Once an incident is detected or reported, the CSU will log the incident in their incident management system and perform a preliminary assessment to determine its nature and severity. This involves gathering initial details about what happened, when it occurred, and the potential impact on operations.

• Incident Recording

- **Documentation**: The CSU team will keep a record of all relevant information about the incident in an incident log. This log will include:
    - **Date and Time**: When the incident was detected and logged.
    - **Description**: A clear and concise description of the incident, including the context and impact.
    - **Category and Severity**: Classification of the incident based on its type (e.g. security breach, system failure) and severity (e.g. minor, major, critical).
    - **Affected Systems/Services**: Identification of the systems, services, or departments impacted by the incident.
    - **Reporter**: Record of the person who reported the incident and any initial actions they took.

- **Initial Actions taken**: Note of any immediate responses or mitigations implemented to address the incident.

• Incident Management

- **Communication**:
  - *For Standard Incidents* the CSU Team will inform all impacted parties of the incident, it's progress and when resolved.
  - *For P1 and Major Incidents* the ICB Digital Lead will ensure that all relevant stakeholders are informed about the incident. This includes internal and external teams and management, depending on the extent of the incident.
- **Incident Escalation**: Where the incident is categorised as P1 or a Major Incident, escalation to the ICB Digital Lead is required. They will alert the ICB Emergency Preparedness Resilience and Response (EPRR) Team to support organisation or system-wide response if appropriate.
- **Incident Resolution Management**:
  - *For standard incidents,* the CSU team will typically liaise with the impacted team and supplier without the need for further escalations.
  - *For P1 and Major Incidents,* the ICB Digital Lead may assign a response team to manage the resolution and to execute any required Business Continuity Plans. They will determine the membership and frequency of any required meetings and assign actions as appropriate. This may include involvement from the ICB EPRR team and external Providers depending on the type of the incident.
- **Tracking and updates**: The CSU team will continuously update the incident log with new information as it becomes available. This includes progress on resolution, changes in impact and any additional actions taken.

• Standing down procedures

- **Resuming normal services:** Once the incident that occurred has been resolved or a workaround is put in place, the stand down procedures begin:
  - *For standard or P1 incidents* that could be resolved using normal business practices, the CSU will inform the main contact within the directorate/service that the issue has been resolved and normal services can resume.
  - *For P1 incidents that require escalation or Major Incidents* the process for closing the incident is as follows:
    - In the first instance, the Incident Manager from the CSU (or a national Incident Manager if the incident affects national services) shall inform the ICB Digital Lead that a resolution has been found and applied.

Commented [NL1]: @Ulrika Crossfield are the numbers here just a formatting error or are we awaiting information? (in which case we just need to call it out please)

Commented [UC2R1]: They don't show up when you view the doc in desktop.....so a formatting issue, but can only see it on the screen when viewing on Teams

        - The ICB Digital Lead will inform the affected business areas/staff members and confirm that normal service can resume.
        - The ICB Staff members will confirm back to the ICB Digital Lead that services are running as normal and the Business Continuity Plan can be evoked. The ICB Staff shall ensure that data collated on paper during the incident is entered into the affected digital system(s).
        - The ICB Digital Lead shall ensure that communication is sent out to all relevant parties informing them that the services are back to normal.

- **Debrief and lessons learned:**
    - *For severe P1 and Major Incidents* the ICB Digital and EPRR team shall hold a debriefing meeting. Three categories determine how quickly after the incident the debriefing should occur:
        - Hot debrief: Immediately after the incident / within 48 hours of stand down.
        - Cold debrief: within 28 days post-incident.
        - Multi - Agency Debrief: within eight weeks of the close of the incident (actual timing will be set by the lead organisation for the response).
    - The ICB Digital Lead will provide a written report to the ICB EPRR Team which:
        - Outlines the incident that occurred and its root cause
        - Confirms the actions taken to respond to it for resolution
        - Details the actions taken to support the continuation of business/services and
        - Details any lessons learned for future incident responses

Roles and Responsibilities including RACI

All ICB and Partner Organisation staff hold responsibilities for ensuring that digital incidents are managed promptly, and the appropriate processes are followed. The following table details the key roles and responsibilities for Digital Incident Management within the BNSSG ICS.

Role	RACI	Activity
CDIO	Accountable	On behalf of the Board, accountable for the execution of the Plan in accordance with the ICB Policy and National Standards
ICB Digital Lead (BC Lead)	Responsible	On behalf of the Accountable Officer, responsible for the execution of the Plan in accordance with the ICB Policy and National Standards. Act as the Key contact during any national incidents
ICB EPRR Lead	Responsible	Support to any major incidents, ensuring the response is managed in accordance with the ICB Business Continuity Plan
ICB Communications Lead	Responsible	Content Development and Distribution
CSU Incident Manager	Responsible	Incident Management
CSU Helpdesk Staff	Influence	Incident investigation and resolution
ICB Staff	Communicated	Execution of Incident Management Process and Business Continuity Plan
Partners	Communicated	Acknowledgement of the incident and execution of local BCPs where relevant

In some cases, the NHS Regional Team will also need to engage in the response to and resolution of the digital incidents. Such incidents include cyber-attacks affecting national systems. The ICB Digital Lead together with the CSU Incident Manager will be the main contact in these instances and will liaise with the regional and national teams on behalf of the ICS and ICB.

Training and Awareness

Further information on training will be provided to ensure awareness of the handbooks and processes. This will include a connection to the ICB EPRR training that is currently undertaken across the ICB.

Section 2 – Digital Incident Handbooks

These Digital Incident Handbooks have been developed to assist users in responding to digital incidents whilst ensuring that correct processes are followed.

They are grouped based on the type of services and systems used. You will find handbooks for the following:

- ICB Corporate Systems
- Connecting Care – Our Shared Care Record
- Primary Care Systems
- ICS Wide Major Incident

Each of the handbooks is structured as follows:

- A brief description of the services in scope
- What process to follow in response to the incident, depending on the incident type
- Key contact details – both during normal working hours and out-of-hours
- The timescales that we work to resolve the incident (held by the EPRR Team)
- Suggested actions that can be taken to ensure continuity of services

The handbooks are owned by the ICB CDIO and managed by the ICB Digital team. If you have any questions or feedback you would like to provide, please contact them directly.

Section 2 Digital Incident Handbooks:

Digital Incident Handbook 001: ICB Corporate Systems

1. Service Description

All of the ICB Corporate Systems are supported by the SCW CSU. This means that in the event of any issues with the ICB digital systems, the CSU Helpdesk should be alerted in the first instance using the standard email address or telephone number.

Once the CSU have completed their triage and if the incident has been classified as P1 or a Major Incident, the ICB Digital Lead will be alerted who will then liaise with the Tactical on-call manager to assess whether the incident can be managed through a Directorate Business Continuity Plan or if the Corporate Business Continuity Plan needs to be activated.

This plan will only be activated when either the scale of the disruption requires strategic management, or if the disruption risks serious damage to critical services, staff, property, or corporate reputation. If the disruption can be managed at a more appropriate lower level, this is the desired approach. Factors that may help when considering if an incident is a widespread or severe disruption are where one or more of the following apply:

• The incident cannot be dealt with through normal operational procedures or the implementation of a limited number of service-specific Business Continuity Plans.

• Existing response arrangements by services are in danger of being or have been overwhelmed.

• A coordinated corporate response is required to deal with the incident.

• An issue is likely to cause widespread disruption to many services.

• An initially small level of disruption containable within one or a small number of service Business Continuity Plans escalates e.g. widespread illness and a reduction in available staffing and resources.

• As a result of the incident there is an impact on business as usual, health & safety, service delivery and/or ICB's finances or reputation.

Directors are responsible for understanding the thresholds for which they need to activate their Directorate plans. They should escalate any issues where they are concerned that service level response arrangements are in danger of being overwhelmed to the Strategic On-Call Director.

2. The Incident Management Process

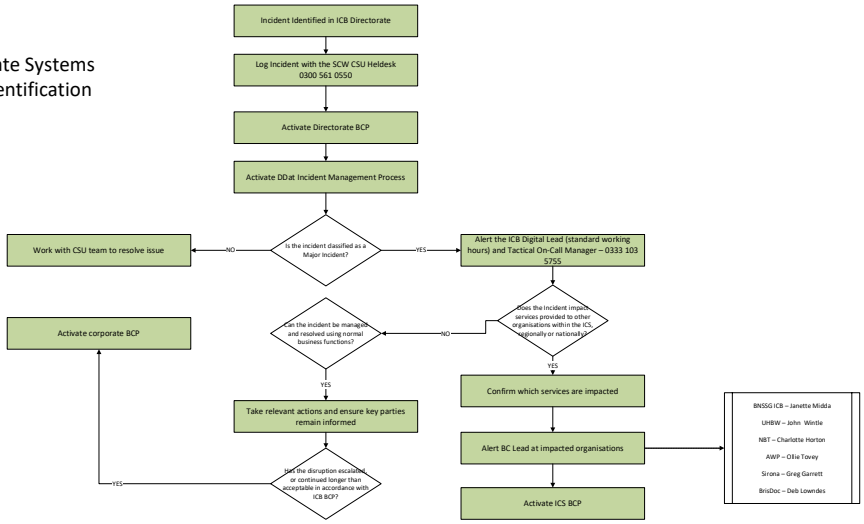
1. Contact SCW CSU helpdesk and log an incident (0300 561 0550)
2. If a standard incident, continue to liaise with the CSU until incident is resolved

3. If categorized as P1 or Major Incident by the CSU
    a. CSU will alert ICB Digital Lead
    b. ICB Digital Lead will assess what action to take and may engage EPRR team
    c. ICB Digital Lead will work with Directorate to determine what Business Continuity Plans are to be activated
    d. Once resolved, normal services will resume and ICB Digital Lead will follow process for debrief and lessons learned

(Action Cards will be available with detailed information)

2.1 Process diagram

ICB Corporate Systems Incident Identification



3. Key contact details

Contacts to be included in internal documentation.

Service/Directorate	Core System	Supported By	Main Business Contact	Phone	Email	Deputy Business Contact	Phone	Email	Alternative Access

1. ICB Digital – Key contacts for escalations

ICB CDIO	
Email	
Telephone	
ICB Digital Lead	
Email	
Telephone	
ICB Director of Integrated & Primary Care	
Email	
Telephone	
ICB Programme Director	
Email	
Telephone	

2. BNSSG ICB Digital On Call Contacts

360 Switchboard	
Email	
Telephone	
BNSSG Tactical On-Call	
Email	
Telephone	
Emergency EPRR	
Email	
Telephone	

System Control Centre	
Email	
Telephone	
BNSSG IT	
Email	
Telephone	
Communications	
Email	
Telephone	

4. Service Levels

SLA's are available within internal documentation.

5. Activities to support continuity of service

ICS Shared Care Record – Connecting Care

1. Service Description

Connecting Care is the local shared care record across the BNSSG ICS. As the name suggests, it is designed to share health and care data across the ICS. The data that is available through Connecting Care is continually evolving.

Connecting Care is accessed either by portal log-in page, or in-context via a source system. If you typically access Connecting Care directly from your primary clinical system and there is an issue with this access, you can request temporary log-in access.

2. The Incident Management Process for Connecting Care

1. Contact SCW CSU helpdesk and log an incident (0300 561 0550)
2. If a standard incident, continue to liaise with the CSU until incident is resolved
3. If categorised as P1 or Major Incident by the CSU:

Commented [NL3]: @Ulrika Crossfield I wasn't sure if the numbering here was correct - starts at 7?

Commented [UC4R3]: @Nicola Lowe - you're right - it's got a formatting error - I'll have a look

Commented [UC5R3]: Now sorted

a. CSU will alert ICB Digital Lead

b. ICB Digital Lead will assess what action to take and may engage EPRR team

c. ICB Digital Lead will work with Directorate to determine what Business Continuity Plans are to be activated

d. Once resolved, normal services will resume and ICB Digital Lead will follow process for debrief and Lessons Learned

(EPRR Action Cards are in development and will be available with detailed information including contact details)

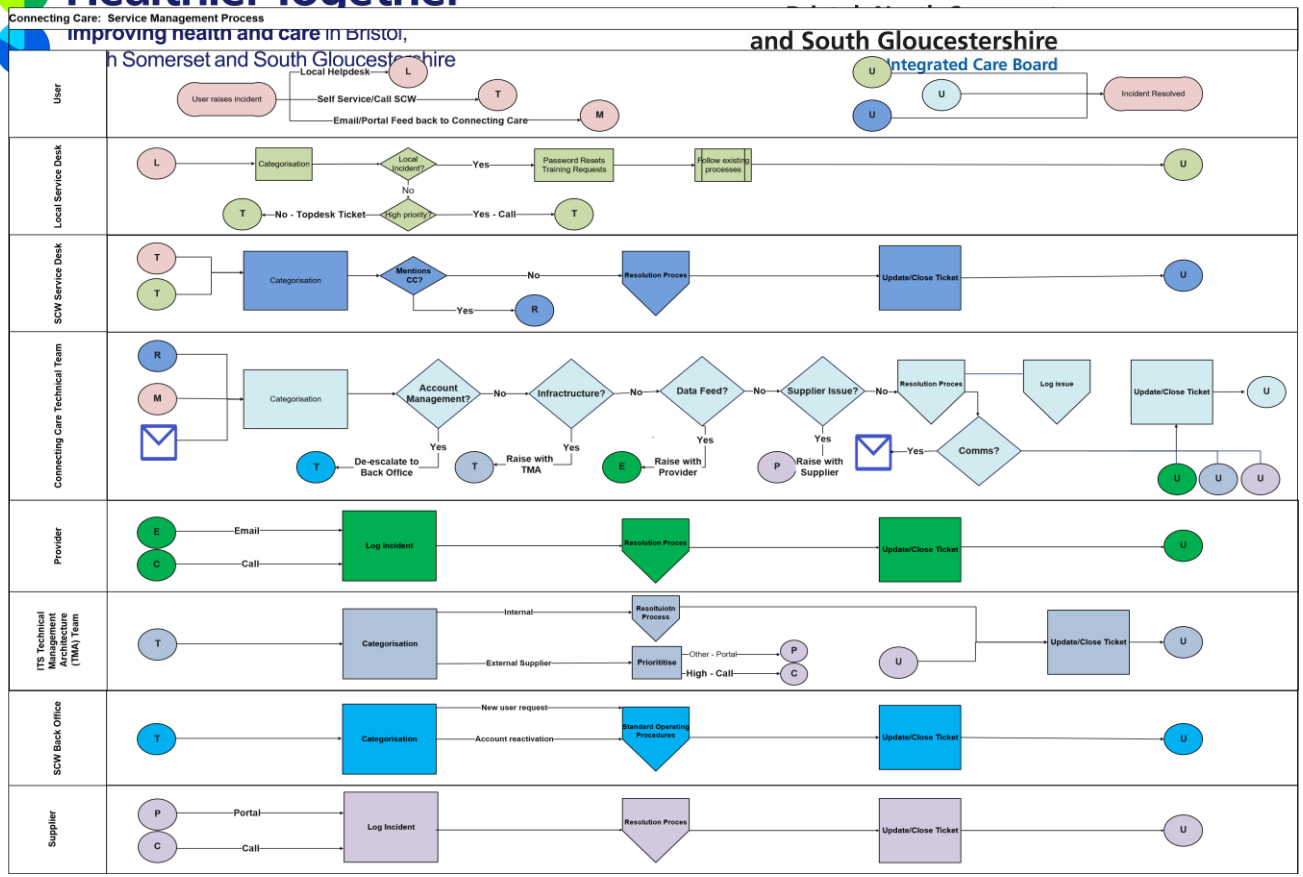
Healthier Together

NHS

Improving health and care in Bristol, and South Gloucestershire

Somerset and South Gloucestershire Integrated Care Board

3.



Digital Incident Handbook 002: Primary Care

1. Service Description

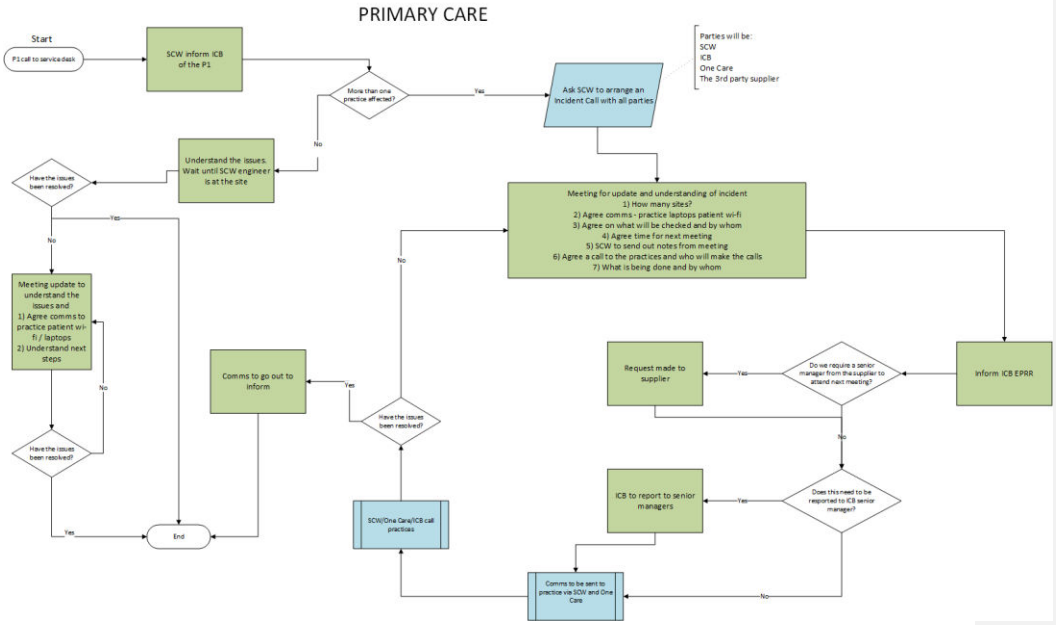
Each of the GP Practices within the ICS are supported by the SCW CSU. The following outlines the process that practices should follow when they identify an issue with their digital services. Depending on the issue and what system is impacted, there are steps that practices can take to ensure that they can continue to provide patient care until such time that normal digital services have been restored.

2. The Incident Management Process

1. Contact SCW CSU helpdesk and log an incident (0300 561 0550)
2. If a standard incident, continue to liaise with the CSU until incident is resolved
3. If categorized as P1 or Major Incident by the CSU:
    a. CSU will alert ICB Digital Lead
    b. ICB Digital Lead will assess what action to take and may engage EPRR team
    c. ICB Digital Lead will work with Directorate to determine what Business Continuity Plans are to be activated
    d. Once resolved, normal services will resume and ICB Digital Lead will follow process for debrief and Lessons Learned

(Action Cards will be available with detailed information)

2.1 Process diagram



Business Continuity Plan – EMIS Patient Record

Below is a guide on how continue to manage patient records during major incidents/outage when unable to access your EMIS records.

Note if the access to EMIS is lost due HSCN connection then practice can connect to the practice Wi-Fi using their laptops to access the full EMIS record.

Patient Record Keeping

1. Activate Business Continuity Mode: If you are using EMIS, switch to Business Continuity (BC) mode immediately. (EMIS Web - Business Continuity in EMIS Web (emisnow.com))
    a. Activate BC Mode in EMIS
        i. Log into EMIS BC
        ii. In session holder filters find your individual staff to see their clinics

iii. Print out essential patient records and distribute them to your staff

2. Print Records: Print off necessary documents and records for your working staff to ensure continuity of care.
3. Local Non-Networked Apps: Utilise Docman or other local applications to pull critical patient information as needed.
    a. Using Docman
        i. Access Docman through your local network
        ii. Retrieve and print critical patient documents as necessary
4. Ensure all team members know how to use Docman to find patient information during the outage.
5. Direct Access to core systems, such as diagnostics data: These will be managed centrally by the SCW CSU/ICB Teams and relevant communication will be provided at the time of the incident
6. Connecting Care: You can access Read Only data on the Shared Care Record from other health and care providers to support decision making. You can so do by requesting a temporary login from the CSU helpdesk
7. Manual Record-Keeping: GP Notes Proforma: Use a simple GP notes proforma to keep records of patient consultations and treatments. Ensure these are detailed and accurate for uploading into the system later when it becomes operational.
        i. Record-Keeping with GP Notes Proforma
        ii. Prepare a standardised GP notes proforma template.
        iii. Use this template to document all patient interactions, treatments, and prescriptions
        iv. Keep these records organised and ready for uploading into your electronic system once it is back online.

Triage Systems

Disable Incoming Triage - Switch off incoming triage systems temporarily to manage the workflow effectively

Disabling Triage Systems:

- Log into your web interface.
- Temporarily switch off the incoming triage system to reduce the influx of new cases
- Inform your staff and patients of this temporary change.

Patient Communication

- Ensure your patients are informed about the outage and its implications.
- Update your practice's website with information about the outage.
- Use social media, email, or SMS to notify patients about potential delays and alternative ways to contact the practice.
- Provide clear instructions on what patients should do in case of emergencies.

Media Enquiries

- Any enquiries from local or national media should be directed to the ICB Business Continuity Lead.

Digital Incident Handbook 003:

Health and Social Care Network (HSCN)

1. Service Description

The Health and Social Care Network (HSCN) is the secure data network for health and care organisations which provides the underlying network arrangements to help integrate and transform health and social care services.

With an increase in systems accessed via networks rather than locally, incidents, where an HSCN connection is lost, will disrupt services.

As these network connections are so critical, the ICB and CSU have robust incident management arrangements in place with the network provider and the CSU will act as the main contact for any incident resolution.

For affected GP Practices, there are ways in which you may potentially still be able to access your web-based clinical systems using your practice Wi-Fi.

2. The Incident Management Process

1. Contact SCW CSU helpdesk and log an incident (0300 561 0550)
2. If a standard incident, continue to liaise with the CSU until incident is resolved
3. If categorized as P1 or Major Incident by the CSU:
    a. CSU will alert ICB Digital Lead

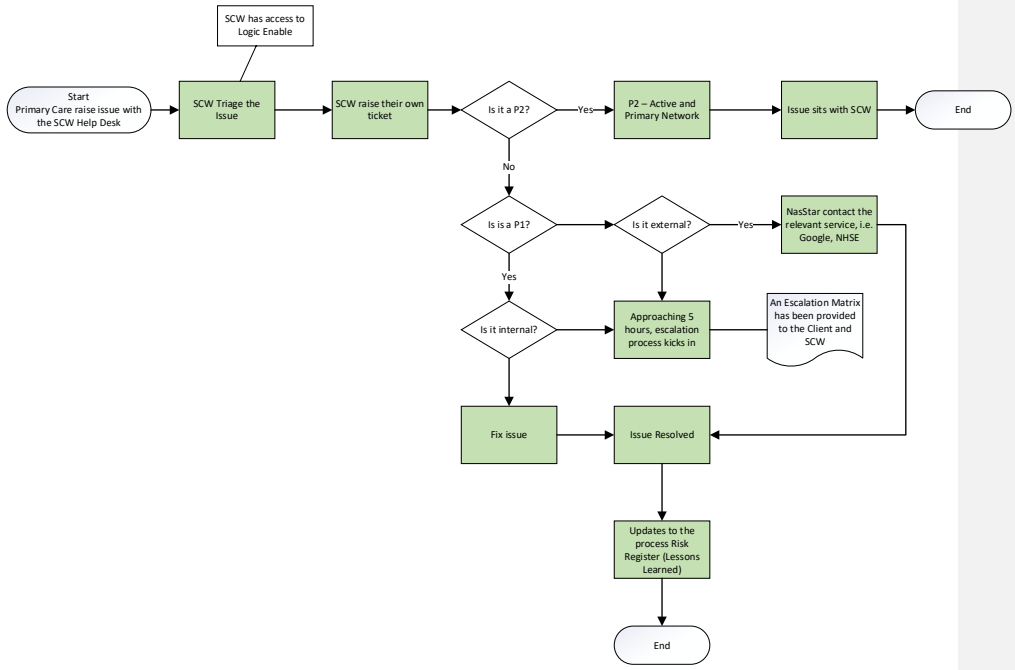
b. ICB Digital Lead will assess what action to take and may engage EPRR team

c. ICB Digital Lead will work with Directorate to determine what Business Continuity Plans are to be activated

d. Once resolved, normal services will resume and ICB Digital Lead will follow process for debrief and Lessons Learned

(Action Cards will be available with detailed information)

4. 2.1 Process diagram



5. The Role of the Integrated Care Board (ICB) in a System-Wide Major Digital Incident

The ICB Board have a duty to ensure that there are robust policies, processes and systems in place to respond to Major Digital Incidents. They will also need to ensure that there are trained, designated resources with responsibilities for Incident Management.

With its central role, during any Major Incident, the ICB will serve as the central coordination and communication hub during an incident.

The designated ICB officer will:

1. act as the main contact to other ICS Partners in response to any system-wide incidents
2. ensure that the ICB EPRR Tactical On-Call Manager and Strategic Director are alerted of the incident
3. actively manage the response until the incident is fully resolved in accordance with the standard operating procedures *(Action Cards will be available with detailed actions for each role)*
4. ensure that all affected ICS partners are promptly informed of the incident
5. set-up the necessary meeting cadence and chair each of the meetings using MS Teams or Conference Call facilities if MS Teams is not available
6. assign resources to complete necessary actions in response to the incident
7. ensure that detailed records are kept of the response to the incident
8. ensure that appropriate stand-down procedures are followed once the incident is resolved
9. schedule and chair the debriefing sessions and provide a post-incident report to the ICB Board with any recommendations for improvements in responding to future incidents

Engagement with any external service providers (whether NHS or Suppliers) will be handled through established contractual relationships to ensure efficiency and effectiveness.

The ICB Communications Team will manage all media relations, ensuring clear and consistent messaging.

Additionally, the ICB Digital Team will maintain a register of interdependencies between organisational Business Continuity Plans (BCPs), particularly where support from other organisations is necessary, such as direct access to specialist systems for test results.

For further guidance, please refer to the ***NHS BNSSG ICB Business Continuity Plan 2023_v0.4*** and ***04_BNSSG_ICB_IRP_November 23 v2.3_Part 1_FINAL***

Contact details to be available within internal documentation.

ICB CDIO	
Email	
Telephone	
ICB Digital Lead	
Email	
Telephone	
ICB Director of Integrated & Primary Care	
Email	
Telephone	
ICB Programme Director	
Email	
Telephone	

6.

7. The Role of the ICS Partners in Responding to System-wide Digital Incidents

The ICS Partners have a duty to ensure that they have established Incident Management Systems in place with trained staff that are fully abreast of their roles and responsibilities during a Major Incident.

The ICS Partners shall ensure that their Business Continuity Plans and Incident Management Plans do not conflict with the ICB Plans. These plans should clearly identify when and how to contact the ICB.

Each ICS Partner shall nominate a designated lead who will serve as the primary contact for the system-wide response team and will represent their organisation in joint meetings. A deputy officer should also be appointed.

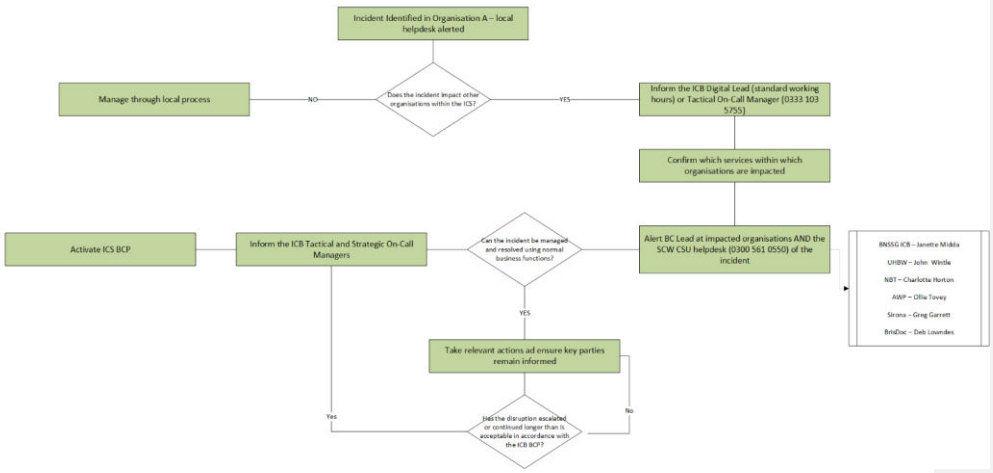
The lead will

1. advise the EPRR Team of the incident promptly confirming the systems impacted and the outcome of any local initial diagnosis
2. assist in the diagnosis of the impact on other organisations
3. participate in any scheduled ICS-wide incident management meetings to ensure there is a coordinated response to the incident between all partners *(Actions Cards will be available with detailed information on what actions to take)*
4. co-ordinate their own organisation's Business Continuity Plan (BCP) and advise the ICB response lead of the actions taken and any plans for resolution
5. ensure that any challenges in executing the organisation's BC plan are communicated to the ICB
6. coordinate all local actions related to the system-wide response
    a. ensuring that local actions align with the agreed system-wide response
    b. providing regular communication to the ICB response lead on actions taken and their impact to the system-wide response
7. conduct an immediate 'Hot debrief' with responding staff once the incident is resolved
8. ensure any records/logs/documents are collected and pass them to the ICB for safe storage
9. attend any further debriefing sessions as directed and contribute to the post-incident report

For further guidance, please refer to the ***NHS BNSSG ICB Business Continuity Plan 2023_v0.4*** and ***04_BNSSG_ICB_IRP_November 23 v2.3_Part 1_FINAL***

2.1 Process diagram

Digital Incident Impacting Multiple Organisations Across the ICS



4. Key Contacts

Contact details to be available within internal documentation.

Organisation	Role	Name	Phone	Email
Bristol, North Somerset & South Gloucestershire Integrated Care Board (BNSSG ICB)	Emergency Preparedness Resilience & Response Manager			
University Hospitals Bristol & Weston NHS Foundation Trust (UHBW)	Emergency Preparedness Resilience & Response Manager			
North Bristol NHS Trust (NBT)	Emergency Preparedness Resilience &			

	Response Manager			
Avon & Wiltshire Mental Health Partnership (AWP)	Emergency Preparedness Resilience & Response Manager			
Sirona Care & Health	Head of Emergency Preparedness, Resilience & Response			
BrisDoc Healthcare Services	Programme and Service Director			

Appendices

Appendix A – SCW CSU DDaT Incident Management Process

8. References

NHS BNSSG ICB Business Continuity Plan 2023_v0.4

04_BNSSG_ICB_IRP_November 23 v2.3_Part 1_FINAL

BNSSG_ICB_IRP_August 22 V1.7 Part 2 FINAL_Incident Coordination Centre Action Cards