Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide
Code: EP10
Issue number: 2

Information Security Incident Response Plan

Lead executive	Director of Operations
Authors details	Emergency Planning and Business Continuity Coordinator

Type of document	Plan
Target audience	All Staff
Document purpose	To effectively manage and respond to information security incidents.

Approving meeting	Emergency Planning Sub-Committee	Date 10/9/19
Implementation date	September 2019	

CWP documents to be read in conjunction with	
IM6	Information Sharing overarching policy
IM7	Code of Confidentiality policy
IM10	Information Governance policy
GR7	Major Incident plan
GR17	Freedom of Information policy
HR3.3	Disciplinary Procedure and policy

Document change history	
What is different?	Incorporating amends following Exercise Trojan 12th August 2019 and feedback from NHS England (changing Action Cards into tabular format)
Appendices / electronic forms	Not Applicable
What is the impact of change?	None

Training requirements	Evaluated as part of the Emergency Planning training and exercise programme.

Document consultation	
Clinical Services	Heads of Operations Acute Care
Corporate services	Jane Thomas/Phil Spencer/Gill Monteith/Jodie D’Enrico
External agencies	Local Health Resilience Partnership/ NHS England

Financial resource implications	None

External references

- NHS Digital Data Security Standard 7 & NHS England
- +69

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? Select		
Is the impact of the document likely to be negative?	No	
- If so can the impact be avoided?	N/A	
- What alternatives are there to achieving the document without the impact?	N/A	
- Can we reduce the impact by taking different action?	N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

Do not retain a paper version of this document, always view policy / guidance documents from the desktop icon on your computer

Contents

1. Introduction

Cheshire and Wirral Partnership NHS Foundation Trust (CWP) must be able to manage and respond to information security incidents supported by clear procedures for reporting, undertaking assessments and defined areas of responsibility.

The purpose of the CWP Information Security Incident Response Plan is to minimise any immediate and long term business impact of any incidents that have the potential to affect the confidentiality, integrity or availability of NHS data and other UK Government information. It enables CWP to react to incidents in a structured and cohesive manner as defined with the CWP Major Incident plan GR7.

In addition CWP's management of an information security incident will include regulatory and legislative reporting and response activities as required by the General Data Protection Regulation (GDPR 2016), the Data Guardian requirements (Caldicott principles, data security standards and data security recommendations) and the National Cyber Security Centre (NCSC) Guidance. These are supported by the following CWP policies;

- IM6 Information Sharing overarching policy
- IM7 Code of Confidentiality policy
- IM10 Information Governance policy
- GR17 Freedom of Information policy
- HR3.3 Disciplinary Procedure and policy
- GR12 Media Relations policy

2. Information Security Incidents

An information security incident is an event, or chain of events, that could compromise the confidentiality, integrity or availability of information. Examples of information security incidents within CWP can include but are not limited to:

- Potential and suspected disclosure of NHS or other Government information to unauthorised individuals
- Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored
- Disruption to systems and business processes
- Inappropriate access controls allowing unauthorised use of information
- Attempts to gain unauthorised access to IT systems
- Records altered or deleted without authorisation by the data 'owner'
- Virus or other malicious (suspected or actual) security attack on IT equipment, systems or network
- Information disclosure obtained by deception
- Breaches of physical security e.g. forcing cabinets, breaking and entering into secure rooms which contain NHS sensitive or other UK Government information
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information
- Human error e.g. emailing data by mistake
- Covert or unauthorised recording of meetings and presentations
- Damage or loss of information and IT equipment due to human failings, theft, fire, flood, failure of equipment or power surges
- Cyber attack
- High severity CareCERT advisory

3. Information / data breach

An information / data breach is a security incident where sensitive, protected or confidential data has intentionally or unintentionally been released or obtained by persons who are not authorised to view or access it.

As CWP handles considerable amounts of personal and sensitive data – person identifiable information (PII), losses of this nature are particularly damaging not only to the service user or person concerned but also to the reputation of CWP and the NHS. Any information / data breaches that relate to PII must be identified as soon as possible to ensure that all regulatory and legislative reporting is discharged immediately.

4. Information Security Incident Reporting

Every CWP staff member is responsible for reporting information security incidents.

Datix incident reporting is the preferred method for all information security incidents. Access to Datix is readily available to all CWP staff members.

If there is a breach of confidentiality or lost / stolen records a Datix form must be completed. Any incidents relating to General Data Protection Regulation / legislation confidentiality issues must be notified to the Trust Records & Information Governance Manager/ Data Protection Officer who will assess the level of breach and report to the Information Commissioner in accordance with NHS Digital's Guide to the Notification of Data Security and Protection Incidents. The aforementioned manager will liaise with the Caldicott Guardian.

Immediately after an information security event occurs the CWP ICT Services should be informed. This should be done by telephone on the following number which is readily accessible and displayed on the desk top of all CWP IT hardware, together with the asset number:

- 0300 303 8182

CWP ICT Services will open a ticket for the incident. Information provided should include:

- Date.
- Location
- Type of incident (e-mail, lost/stolen device etc).
- Short summary of what occurred.
- Impact on multiple or single users and/or sites.
- Mitigating steps taken (if any).
- Datix reference number.
- Contact details for further information.

5. Information Security Incident Analysis and Response

All reported information security incidents will be assessed as soon as possible so that the most appropriate course of action and a priority can be assigned to support resolution. Incidents will be rated for urgency as high, medium or low as shown in the table 1 below:

Table 1

Category	Description
High (H)	The damage caused by the incident increases rapidly. Work that cannot be completed by staff is highly time sensitive. A minor incident that can be prevented from becoming a major incident by acting immediately. Several users with VIP status are affected.
Medium (M)	The damage caused by the incident increases considerably over time. A single user with VIP status is affected.
Low (L)	The damage caused by the incident only marginally increases over time. Work that cannot be completed by staff is not time sensitive.

Incidents will be further assessed and categorised according to their likely impact as shown in the table 2 below:

Table 2

Category	Description
High (H)	A large number of staff are affected and are not able to do their job. A large number of service users / patients are affected and there is a serious risk of harm. The financial impact of the incident is likely to exceed £10,000. The reputational damage to CWP and the health service is likely to be high.
Medium (M)	A moderate number of staff are affected and are not able to do their job. A moderate number of service users / patients are affected and there is a reduction in the delivery of care. The financial impact of the incident is likely to exceed £1,000 but not £10,000. The reputational damage to CWP and the health service is likely to be moderate.
Low (L)	A minimal number of staff are affected and / are able to do their job but this requires extra effort. A minimal number of service users / patients are inconvenienced but safe and effective care continues. The financial impact of the incident is not likely to exceed £1,000. The reputational damage to CWP and the health service is likely to be minimal.

Once an incident has been categorised against urgency and impact, priority will be agreed by reference to the incident priority matrix as shown in table 3:

Table 3

		Impact		
		H	M	L
Urgency	H	1	2	3
	M	2	3	4
	L	3	4	5

Priority codes will be utilised to identify the specified target response and target resolution times as shown in the below table:

Table 4

Priority	**Description**	**Target Response Time**	**Target Resolution Time**
1	Critical	Immediate	1 Hour
2	High	10 Minutes	4 Hours
3	Medium	1 Hour	8 Hours
4	Low	4 Hours	24 Hours
5	Very low	1 Day	1 week

Dependant on the type of information security incident, the CWP Head of ICT Services and / or the Trust Records and Information Governance Manager / Data Protection Officer will be notified immediately. These roles will lead the analysis of the incident which will include the following:

- Identification of the type of incident
- An assessment of the severity of the incident
- An assessment of the scale in terms of data size, e.g. Gb of data, number of pages lost, distribution list or impact on multiple or single users and/or sites
- Identification of classification of type of data
- Identification of whether the information is PII
- Identification of criminal activity

The decision making process will be recorded either electronically or on paper. If the data breach is identified as PII the Caldicott Guardian and Communications team must be informed.

Following analysis, escalation of the information security incident must be considered. Any escalation undertaken must take account of internal and external escalation pathways and regulatory requirements.

Internal escalation should consider (this is not an exhaustive list):

- The Caldicott Guardian
- The Senior Information Risk Owner
- The Director of People and Organisational Development
- The on call 3rd Tier Executive
- Head of Communications and Engagement
- The Emergency Planning Team

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- The Local Security Management Specialist
- All staff

External escalation should consider (this is not an exhaustive list):

- NHS Digital Data Security Centre
- NHS England/ NHS Improvement
- The Information Commissioner
- Department of Health
- Clinical Commissioning Groups
- NHS Trusts
- Law Enforcement
- National Cyber Security Centre (NCSC)
- Cheshire & Merseyside Cyber Security Group

The analysis will identify the appropriate and proportionate response to the incident. This will include whether the response should include the declaration of:

Business Continuity Incident	An event or occurrence that disrupts, or might disrupt, CWP's normal service delivery, below acceptable predefined levels, where special arrangements are required to be implemented until services can return to an acceptable level.
Critical Incident	Any localised incident where the level of disruption results in CWP temporarily or permanently losing its ability to deliver critical services, patients may have been harmed or the environment is not safe requiring special measures and support from other agencies, to restore normal operating functions.
Major Incident	Any occurrence that presents serious threat to the health of the community or causes such numbers or types of casualties, as to require special arrangements to be implemented by hospitals, ambulance trusts or primary care services and health organisations.
Data Security Major Incident	An incident that affects public confidence in the NHS resulting in national or international media interest. A significant operational issue that may have implications wider than the remit of one region. An incident that threatens the security of the NHS. An incident that poses a large scale or life-threatening risk to patient safety.

Once the analysis has been completed a response will be co-ordinated and implemented. The response will identify a number of activities which will include the following:

- Date, time, type and location of the incident.
- Declaration of the incident.
- Identification of who is leading the response.
- Identification of will be supporting the response.
- Where the response will be managed from.
- Identification of the impact.
- Identification of stakeholders involved and /or impacted.
- Recording of all decisions and actions.
- The communication strategy.
- Evidential preservation.

If a national major incident is declared, NHS England will lead in line with existing Emergency Preparedness Resilience and Response (EPRR) processes.

6. Collection of Evidence

CWP will ensure that if an incident is suspected of being caused by a criminal act or if legal action is anticipated, steps are taken to ensure that any evidence necessary to support an investigation and successful prosecution is not intentionally or accidentally destroyed. Advice can be sought from the NHS Digital Data Security Centre.

7. Learning from Incidents

A post incident investigation of the information security incident and the actions taken to resolve the incident will be undertaken to:

- Determine the root cause of the incident
- Quantify the impact on CWP, partners and stakeholders
- Minimise the possibility of a recurrence
- Improve future responses
- Refresh training and awareness
- Review contractual and service level agreements

A report will be prepared as early as possible into the incident to qualify the severity of the incident and outline the proposed response and investigative activities. The report should be presented to the CWP Executive Team for endorsement of the proposed response and investigation activities.

Upon completion of the full analysis, response and investigation elements, a draft report should be produced and reviewed by all the relevant stakeholders before being finalised and entering the CWP governance mechanism.

The report should include the following:

- Summary of the incident
- Responses undertaken
- Findings of the investigation
- Onward reporting requirements
- Further follow-on actions
- Lessons identified

8. Follow on Actions

Following the assessment of the lessons identified follow-on actions may be required to:

- Update or change the incident response process
- Update or change ICT system configurations either hardware or software which should be managed through the CWP change management governance process
- Update or design training either for all CWP members or specifically for identified roles
- Change policies, operating procedures, standards or guidance or introduce new ones to reduce the risk of that type of incident reoccurring
- Communicate learning via *Shared Learning* bulletin or via normal internal communication channels

9. Testing

Regular testing of the Information Security Incident Response Plan is required to ensure it remains fit for purpose. Any invocation of the plan for 'real' will discount the need for testing. In line with CWP EPRR practice the following testing of the plan will take place:

- Table top exercise – annually
- Live test – every 3 years

10. Appendix: Action Cards

ACTION CARD – Head of ICT Services	
Role	To regularly assess the incident and ensure the appropriate response is implemented.
Reports to	Trust Incident Officer

ACTION	Completed (time) ✔
1. Report to the **Trust Incident Officer** and agree from which location(s) you will respond to the incident – it may be ineffective to be situated in the incident room	
2. Present a severity assessment	
3. Agree a communication process with the Trust Incident Officer	
4. Ensure all decisions and actions are recorded	
5. Contact NHS Digital Data Security Centre	
6. Present timely relevant information for Sitreps	

At the end of your shift you may hand over to someone else. Please make sure that you hand this action card to them. Make sure they know what arrangements are in place for storing records etc.

You may be working on a rota to cover a 24 hour period. Given the intensity of the work, you should ensure that you take regular short breaks to relieve stress and clear the mind.

ACTION CARD – Records and Information Governance Manager/ Data Protection Officer	
Role	To regularly assess the incident and ensure the appropriate response is implemented.
Reports to	Trust Incident Officer

ACTION	Completed ✔ (time)
1. Report to the **Trust Incident Officer** and agree from which location(s) you will respond to the incident – it may be ineffective to be situated in the incident room	
2. Present a severity assessment	
3. Agree a communication process with the Trust Incident Officer	
4. Ensure all decisions and actions are recorded	
5. Contact the Caldicott Guardian	
6. Contact the Senior Risk Information Officer	
7. Liaise with the Local Security Management Specialist	
8. Present timely relevant information for Sitreps	

At the end of your shift you may hand over to someone else. Please make sure that you hand this action card to them. Make sure they know what arrangements are in place for storing records etc.

You may be working on a rota to cover a 24 hour period. Given the intensity of the work, you should ensure that you take regular short breaks to relieve stress and clear the mind.

ACTION CARD - Executive on-call / Trust Incident Officer	
Role	To set up appropriate level of response
Reports to	Chief Executive

ACTION	Completed ✔ (time)
1. Keep a record of all messages received or given. Use the personal log sheet in **Executive On-Call Pack and r**ecord: • Date/ time • Name of caller • Contact details phone/ fax • Outline of message • Actions taken	
2. Use **Severity Assessment**	
3. Identify location for management of the incident. Assemble the resources required to respond to the incident. Confirm: • What has happened • Where • What is being done to address the incident • What actions need to be taken and by whom • Agree process for Sitreps	
4. Contact the **NHS England Cheshire and Merseyside Area Team** and inform them of the current situation. Confirm: • What has happened • Where • What is being done to address the incident • What actions need to be taken and by whom If necessary call the North West Ambulance Service Regional Operations Co-ordinating Centre (ROCC) on 0345 113 0099	
5. Inform the **Chief Executive** and **Chairman** of the situation	
6. Inform Trust **Head of Communications**	
7. Call the **Emergency Planning Team** and ask him/her to call admin support staff and open up and prepare the incident room	
8. If necessary, call other **senior officers** to be members of the incident management team, brief them on the situation and ask them to report to the incident room.	
9. If necessary, move to the major incident room.	
10. Liaise closely with **Decision Loggist** to record all decisions taken	
11. If you need to set up a teleconference use: • Dial in number: **0844 737373** Pin: **277403** • Short code for a mobile: **87373** and pin when prompted **277403**	

At the end of your shift you may hand over to someone else. Please make sure that you hand this action card to them. Make sure they know what arrangements are in place for storing records etc.

You may be working on a rota to cover a 24 hour period. Given the intensity of the work, you should ensure that you take regular short breaks to relieve stress and clear the mind.

ACTION CARD – Emergency Planning Team	
Role	To support the Trust Incident Officer To support the incident team
Reports to	Trust Incident Officer

ACTION	Completed ✔ (time)
1. Agree role with **Trust Incident Officer**. You may be undertaking more than one role.	
1 Set up incident room • Confirm room layout, communications and management systems • Confirm message handling system • Set up and maintain incident status boards	
2. Agree frequency of team meetings and Sitreps with **Trust Incident Officer**	
3. At first team meeting confirm your role, which is: • To ensure that team members follow established communications procedure: as per their respective action cards • Manage the incident room • To use separate phones for incoming and outgoing calls (do not tell anyone your outgoing number) • To record key contact numbers on status board/flip chart • To maintain a watching brief on issues management i.e. to ensure that correct links with in-house and external partners are being maintained • To establish and maintain contact with any other emergency centres. To brief these centres on progress of actions taken by the Trust and to obtain updates from them.	

At the end of your shift you may hand over to someone else. Please make sure that you hand this action card to them. Make sure they know what arrangements are in place for storing records etc.

You may be working on a rota to cover a 24 hour period. Given the intensity of the work, you should ensure that you take regular short breaks to relieve stress and clear the mind.

ACTION CARD – Decision Loggist	
Role	To maintain a contemporaneous record and documentation of all decisions taken by the Executive On-Call/Trust Incident Officer
Reports to	Emergency Planning Team

ACTION		Completed ✔ (time)
1	Report to the **Trust Incident Officer** and confirm your role as follows: • Meet with Executive On-Call/Trust Incident Officer • Keep all contemporaneous records and documentation of decisions • Note date, time, place of any meetings and those attending • Note brief summary of incident • Record decision made, by whom and rationale for the decision • Ensure record is signed and time noted of start and finish of meeting	

At the end of your shift you may hand over to someone else. Please make sure that you hand this action card to them. Make sure they know what arrangements are in place for storing records etc.

You may be working on a rota to cover a 24 hour period. Given the intensity of the work, you should ensure that you take regular short breaks to relieve stress and clear the mind.

ACTION CARD – Head of Communications and Engagement	
Role:	Give advice on all aspects of handling media
Reports to:	Associate Director of Communications and Engagement

ACTION	Completed ✔ (time)
1. On receiving the information that an incident has been declared staff should inform the Associate Director of Communications and Engagement. Ensure the rest of the team has been briefed. Dependant on incident and availability one of the communications leads will support the major incident room whilst the other supports the communications office.	
2. Liaise with NHS England Cheshire and Merseyside Area Team/ NHS Improvement on key communications issues	
3. Liaise with communications office and feedback to major incident room on any developments	
4. Set up a media briefing room (if needed) with support from Communications team, NHS England and Engagement, and the Police Bronze Press Officer at the scene (if incident on CWP property)	
5. Write briefings to keep staff partners and stakeholders updated	
6. Oversee Communications team in drafting press releases / media briefings	
7. Approve press releases / media briefings	
8. Oversee issue/distribution of approved press statements	
9. Flag urgent media enquiries	
10. Oversee communications team in updating website / intranet / any social media CWP channels	
11. Oversee calls to the communications office and flag any calls of importance to major incident room	

Key issues checklist (questions)

- **What is the information security incident and what are the implications?** What precisely has happened? Do we all have the same understanding of the situation?
- **Is there a more fundamental problem?** Could this be the tip of the iceberg? How could this incident call into question the reputation of the whole organisation/NHS? How could this become a broader issue?
- **Is there more to come?**
- **What is the worst case?** How much worse could it get?
- **What is actually at stake?** What could we lose if it gets worse, will our stakeholders stay with us through this crisis? Are we panicking unnecessarily? Is there something at stake here that we haven't thought about yet?
- **What are the audiences likely to make of it?** Stepping outside the potential crisis – what would it look like from the outside? What would the local community, members, politicians, media etc, make of it? Could we sound out some people for their initial reaction?
- **What are the likely timescales?** How long is there before the deadlines of the various media involved? Is the holding statement all we have time for or could we issue something else with more detail? And by when should we have communicated with other stakeholders? How long is the crisis likely to run?
- **Can any allies be brought in?** Would our messages be more credible coming from a third party? Would they speak out on our behalf?
- **Who else is involved?** Regulatory bodies, government, Police etc. This could affect strategy. Should we partner with another organisation to handle it jointly?
- **How can the crisis be contained?** How can our actions now put a lid on this as quickly as possible preventing speculation/negative publicity from spreading?

At the end of your shift you may hand over to someone else. Please make sure that you hand this action card to them. Make sure they know what arrangements are in place for storing records etc.

You may be working on a rota to cover a 24 hour period. Given the intensity of the work, you should ensure that you take regular short breaks to relieve stress and clear the mind.