Document Details	
Title	**IG02 – Process for Handling Data Protection Breach**
Author	CIC Board
Quay Primary Healthcare CIC ref no:	IG02
Version	1.5

Approval process	
Approved by	CIC Board
Date approved	04 December 2015
Lead Director	Medical Director
Category	**Information Governance**
Sub Category	**Information Governance**
Next Review Date	15 Feb 2024
Superseded document (If applicable)	

Distribution	
Who the policy will be distributed to	All Quay Primary Healthcare CIC Team
Method	Email

Version Control		
No:	Date	Amendment
1.1	Feb 2017	Lead Director – updated details
1.2	16 05 2018	Revised in preparation for GDPR
1.3	16 May 2020	Policy review and revision – change of organisation name
1.4	25/11/2021	Change of organisation name – Quay Primary Healthcare CIC

1.5	15/2/2023	Updated to confirm, individuals must be informed of any breach of their personal information.

IG02 – Process for Handling a Data Protection Breach

Contents

1. Dealing with a Breach

In the event of a breach leading to disclosure, it is important that Quay Primary Healthcare CIC respond appropriately.

Quay Primary Healthcare CIC should ensure that any breach response considers:

Containment and recovery

Assessment of ongoing risk

Notification of breach

Evaluation and response

2. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.

Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.

Establish whether there is anything Quay Primary Healthcare CIC can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backup tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

Where appropriate, inform the police.

3. Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the business.

While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, Quay Primary Healthcare CIC should assess the risks which may be associated with the breach. The most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

To make this assessment, Quay Primary Healthcare CIC should consider:

What type of data is involved?

How sensitive is it? Some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)

If data has been lost or stolen, are there any protections in place such as encryption? Are there lessons for the future here?

What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk

Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people

How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment

Who are the individuals whose data has been breached? Quay Primary Healthcare CIC holds personal data for staff and others as well as patients

What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service Quay Primary Healthcare CIC provide?

If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help Quay Primary Healthcare CIC prevent fraudulent use.

4. Notification of breaches

Informing people and organisations of a data security breach can be an important element in the breach management strategy. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. Since 26 May 2011 information service providers have had have a requirement to notify the ICO, and individuals themselves, of personal data security breaches. If they are acting as data processors on Quay Primary Healthcare CIC's behalf this may impact on the organisation

Quay Primary Healthcare CIC should consider the following questions in deciding whether to notify:

Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances, in other areas sector specific rules may lead Quay Primary Healthcare CIC towards issuing a notification.

Can notification help Quay Primary Healthcare CIC meet its security obligations with regard to the seventh data protection principle?

Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information Quay Primary Healthcare CIC provide to mitigate risks, for example by cancelling a credit card or changing a password?

If a large number of people are affected, or there are very serious consequences, Quay Primary Healthcare CIC should inform the ICO.

Consider how notification can be made appropriate for particular groups of individuals, for example, if Quay Primary Healthcare CIC is notifying children or vulnerable adults.

Quay Primary Healthcare CIC must notify the appropriate regulatory body. The ICO should only be notified when the breach involves personal data

The notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what Quay Primary Healthcare CIC has already done to respond to the risks posed by the breach

When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what Quay Primary Healthcare CIC is willing to do to help them

Provide a way in which they can contact Quay Primary Healthcare CIC for further information or to ask questions about what has occurred – this could be a helpline number or a web page, for example.

When notifying the ICO Quay Primary Healthcare CIC should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures Quay Primary Healthcare CIC had in place at the time the breach occurred. Quay Primary Healthcare CIC should also inform the ICO if the media are aware of the breach so that we can manage any increase in enquiries from the public.

When informing the media, it is useful to inform them whether Quay Primary Healthcare CIC have contacted the ICO and what action is being taken. The ICO will not normally tell the media or other third parties about a breach notified to us, but they may advise Quay Primary Healthcare CIC to do so.

The ICO has produced guidance for organisations on the information they expect to receive as part of a breach notification and on what organisations can expect from them on receipt of their notification.

It is available on their website at:
https://ico.org.uk/for-organisations/guide-to-data-protection/ principle-7-security

5. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of Quay Primary Healthcare CIC's response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if Quay Primary Healthcare CIC's response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

6. GDPR

We acknowledge that GDPR is effective from 25th May 2018 and impacts on changes to data protection legislation, however we await the final Data Protection Act 2018 to be released in order that we can attain guidance from the Codes of Practice from the Information Commissioners' Office and the Information Governance Alliance *(part of NHS Digital)*.

7. Summary of response

1. Containment and recovery

Immediate Actions:

- Confirm breach
- Inform SIRO and Caldicott Guardian
- Appoint SIRO and/or CG to lead response
- Identify staff who need to know about the breach
- Assign urgent containment actions
- Establish any possible actions to recover any losses and limit the damage
- Where appropriate, inform the police or other third parties eg banks if financial data has been lost

2. Assessment of ongoing risk

Assess potential harm to patients, staff and WHP

- What type of data is involved?
- How sensitive is it?
- Is lost or stolen data protected by encryption? Are there lessons for the future here
- Is data lost, stolen or damaged?
- What could the lost data tell a 3rd party?
- How many people are affected?
- What harm can come to those individuals?
- What are the wider consequences?

3. Notification of breach

Notify those affected and those who need to know. Consider:

- Are there any legal or contractual requirements?
- Does notification help meet security obligations?
- Can notification minimise harm to the individual?
- Does the breach require notification to the ICO? https://ico.org.uk/for-organisations/guide-to-data-protection/ principle-7-security/
- How to notify vulnerable groups appropriately?
- How can affected individuals contact WHP?
- How to notify the media

4. Evaluation and response

Evaluate the effectiveness of WHP's response as well as the causes of the breach:

- Identify underlying causes
- Look for systemic failures
- Identify lessons to be learnt
- Review training needs assessments
- Review training procedures
- Review lines of responsibility