Infographic storyboard: Accidental Internal Breach

Co-created by the public, Kohlrabi and UPD

NOTE: this draft resource specification is intended to be a jumping off point for further shaping by feedback from stakeholders and designers.

Summary of findings guiding the resource development

Design/format: Dialogue participants overwhelmingly preferred storytelling to bring health data security issues to life with relatable experiences. In response, co-creation workshop participants were provided with draft scenarios to develop into relatable stories, explaining security processes, breaches, and responses.

Information level: Many participants realised that they knew less about this subject than they had thought. They requested **basic information** about health data security upfront, with the option to access more in-depth information via signposting supplementary materials.

Visual presentations: A headline animation and interactive infographics were chosen to support the construction of visual understanding, and for accessible, self-paced exploration.

Honest: All participants reported their need for clearer, more honest information about health data security to empower and restore trust. They particularly wanted honesty about what the risks are when breaches occur.

Presentation of risk: There was understanding that risk is everywhere, that it is hard to put a number on breaches or clarify individual impacts. Acceptance of this must be balanced by clear evidence that those responsible for protecting data are present and take their duties seriously.

Key information: What is health data and why is it collected; Access: who is allowed to access; Sharing: How is health data shared within and between direct care staff and health services; What is a breach, who defines it and how to be aware that one has occurred; What are the harms of a breach; Steps to take in case of a health data breach

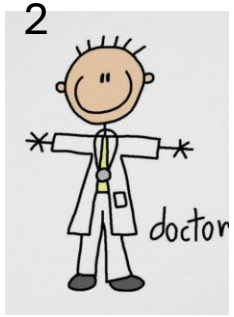
Summary of design decisions:

Overall, it's important that it's a story, relatable, moving through someone's journey, not a PowerPoint brought to life

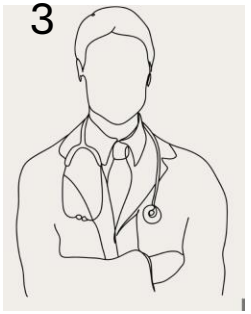
- **Tone:** Serious. It’s a serious issue, so not too playful. Realism- Not just a PowerPoint , properly moving through the story
- **Character design:** range of demographics to ensure relatable, 2D, no. 8. on real scale below, show emotions in expressions, all clearly different people. Healthcare workers wear calming, trustworthy colours (blues/whites), patients wear colours.
- **Detail cues:** Realism whether hospital or home, but muted to remove clutter and put focus on central characters
- **Sound:** Natural noises to accompany the visuals, for example the sound of a keyboard tapping, or ‘data’ whirring, or a whoosh of an email. No strong feelings about light background music either way, but it would need to fit the principles of staying relatable, while balancing between honesty, i.e not playful or upbeat, and conveying a sense of safety, reassurance, and gravitas of the topic.
- **Narration:** No final absolute steer for accent or gender but agreement that diversity is important (include a couple of voices), and suggestion to range Britain e.g. Welsh, English etc to ensure accessibility and maintain interest through variety.
- **Script:** Anywhere that text can be chunked and broken down, do it!
- **Length:** No more than 3 minutes for animation, or moving through infographic.

1

2



3



4

5

6

7

8

9

How to use this material

- Interactive infographics for case study: The slides consists of 'case studies', each of which will be developed into an interactive infographic. In this section, the pop-up text is what will ‘pop up’ as the viewer scrolls through over a graphic.

Background

- The participants discussed a few options for the format of the infographic. They spent time exploring each on this webpage. https://www.ceros.com/blog/interactive-infographic/
- They particularly liked this one where the viewer slides through at their own pace, with options to interact and click for more https://www.ceros.com/inspire/project/goodwin-moderna-history

Scenario 1: **Accidental Internal Breach**

Script & Storyboard

Accidental internal breach infographic: Scene 1

Pop up text:
“Amir recently had surgery and was being cared for by Dr Jackson in the surgical care unit".

Visuals: Introduction to Amir’s Recovery

- Amir (male, mid-40s, medium brown skin tone, short beard) is shown in a hospital bed, recovering from surgery. He is in a hospital gown with an IV line in his arm.
- Doctor Jackson is wearing scrubs with a stethoscope, different demographics to the next doctor.
- **Background**: A clean hospital room, with a blue and white color scheme, a heart rate monitor, and a window with daylight filtering in.

Accidental internal breach infographic: Scene 2

Pop up text on Amir:
"He has now been discharged to Dr Williams in outpatient services so that he can continue to have check-ups while he recovers."

Pop up text on Dr: "Dr Williams has some questions about the surgery to make sure she gives Amir the best care. She writes her questions in an email, some of which refer to sensitive information from Amir's medical record, and sends it over to Dr Jackson."

Visual: Transition to Outpatient Care

- Amir is in waiting room, wearing casual clothing now. The outpatients sign is visible behind Amir.
- Move to a split screen (room next door to waiting room): Dr. Williams Drafting an Email
- Dr. Williams (Black woman, 50s, glasses, professional attire, stethoscope) is sitting at her office desk, typing an email on a computer. Her office is a medical office, with bookshelves, posters, and stacks of paperwork.

- **Participants suggested more plain language, less fussy text:** Consider *Dr. Williams has some questions about Amir's surgery and emails Dr. Jackson for more information*.

Accidental internal breach infographic: Scene 3

Pop up text: “However, she accidentally sends it to the wrong colleague- someone else with the same name in the same hospital."

Visual: The Accidental Email Mistake

- Close-up of the computer screen showing the email being sent to the wrong colleague. The recipient list includes *Dr. Jackson (Dermatology)* instead of *Dr. Jackson (Surgery)*. (take out **doctor** if following expert feedback below, could be a different first name?**)**
- **Background**: A busy inbox, with a red exclamation mark next to "Sent."

Pop up text: "The recipient realises what's happened, deletes the email, and contacts Dr Williams to inform them immediately . ”

Visual: The Wrong ~~Dr.~~ Jackson Receives the Email

- **Visual**: A different ~~Dr.~~ Jackson (White man, 60s, bald, glasses) is shown at his computer, opening his email inbox. He sees the subject line referencing Amir's surgery and realizes it is not meant for him.
- **Background**: A dermatology office with posters of skin conditions, a patient chart on his desk, and an open laptop.
- **Note:** Participants added the word **immediately** here, coupling reassurance with breach.

Expert feedback: The example was that she sends it to the wrong Dr Jackson. Feedback was that it could instead be someone else within the organisation with the last name “Jackson”, to reinforce that not only doctors, but all staff within the health organisation, uphold the law and follow data security procedures for deleting emails that are sent to them in error. Consequently, could the visual portray another staff member not a doctor? It could be one from the animation, such as the staff member taking blood, or any other staff member who has been designed by the participants at some point.

Accidental internal breach infographic: Scene 4

Pop up text: Dr Williams reports the incident- which is also known as a data breach - to hospital administration. She sends the email to the right Dr Jackson to ensure Amir gets the right care.

Visual: **Dr. Williams Reacts to the Mistake**
Dr. Williams, looking worried and embarrassed, on the phone to the hospital people, same office setting as before, looking at her screen showing emails with the mistake. Depict 'human face' of hospital responsibility, with there being a responsible staff member depicted on the phone asking as a visual check list which appears line by line coming out the phone:

- "Did you deal with it quickly?"
- "Was only one patient affected?"
- "Do you know that the recipient didn't read the email?
- "Do you know that they deleted the email?"
- "Did you correct the mistake, by emailing the right recipient?"

Expert feedback: The text was, 'Dr Williams reports the breach to hospital administration'. Feedback was that the word "Breach" requires a definition of what that means. They suggested a word update which has been done.

Accidental internal breach infographic: Scene 5

Pop up text: “This is an example of an accidental internal breach – Amir's health data has accidentally been put at risk within the hospital in which he has been cared for.

The Information Commissioner's Officer, or ICO - who regulate and enforce data protection laws in the UK – support organisations to complete a risk assessment after discovering a personal data breach. "

Visual: The ICO staff from the animation is in their office holding the guidance on breach risk assessments. Each step is revealed in turn.

Step 1: Check if personal information is involved
Step 2: Establish what type and how much personal information
Step 3: Consider who might have the personal information
Step 4: Work out how many people might be affected
Step 5: Consider the impact the breach might have on people’s lives
Step 6: Document everything you know about the breach
Step 7: Assess the risk to the people whose information might have been breached

Signpost: hyperlink to ICO webpages on risk assessment

Accidental internal breach infographic: Scene 6

Pop up text: "The risk assessment shows that there is an unlikely risk of harm or detriment to Amir. Therefore, there is no legal obligation for Dr Williams to report the breach to the ICO or to inform Amir that this happened.

However, the ICO recommends that the hospital earns from this incident and that action is taken to prevent against these type of mistakes happening in the future."

Visual: Doctors William and Jackson shown in front of other staff about the incident, in a training session. A conference room with a presentation slide that reads Best Practices for Data Security. The suggestion is that they are teaching their colleagues, within an open culture of learning from mistakes.

Visual: if there is space on the screen, ideally the ICO character would be depicted as if the pop up recommendation about training is coming from them.

Note: The experts consulted in the research underlined that for the ICO it isn't just about the breach but making changes for the future, therefore this storyline has been expanded since the co-creation workshops.

Expert feedback: The text did read 'little risk of harm'. The feedback suggested updating this to 'unlikely risk', a change which has been made. The research team agreed with the explanation that there is an obligation to report a breach to the ICO when there is a *likely* risk to the data subject, whether the risk is little or big doesn't matter, it's the fact that there is likely to be some consequence (even if the consequence isn't that bad).

Accidental internal breach infographic: Scene 7

Pop up text: “Where the risk to you is judged to be low, you may not know that a breach has happened to your data"

This can still be worrying to think about, but in this instance, there is nothing you need to do.

"However, if you have any concerns, you can get support from the ICO on what to do." **Click here to learn more**

Visual: Amir at home on the sofa. He is well. He is content, lightly smiling.

Accidental internal breach infographic: Scene 8

Pop up text: **“**However, if there had been a likely high risk to Amir, for example if Dr Williams had accidentally emailed sensitive information to a group of individuals outside of her organisation, she would have had to report it to the ICO within 72hrs and to notify Amir.

If a breach like this happens to your data and there is a likely high risk to you , you will be notified by the service, such as the hospital or GP practice, with information about what occurred and the process for what happens next."

Visual: Staying with Amir, same scene but he's now on the phone being notified, looking downcast/confused, but being given a clear notification in speech issuing from the phone

Signpost: To learn more about the risk assessment of breaches, click here.
Note: the participants did not know what the patient would be *told*. Subject matter experts may want to add wording here about the process for what happens next

Expert feedback: The text did read: “However, if the risk had been higher, for example if Dr Williams didn't know what the recipient had done with the email, she would have had to report it to the ICO within 72hrs and to notify Amir. ” The feedback was to update the text with their suggested wording (which has been done), because it wasn’t realistic. The scenario– a doctor accidentally emailing someone within their own organisation and them not replying – would not meet the threshold for reporting to the ICO, nor notifying Amir. To report to the ICO, the breach has to be *likely to result in a risk* to the rights and freedoms of the data subject. The bar for notifying data subjects is even higher – it has to be assessed as ***likely*** *to result in a* ***high*** *risk* to them. Incidents may therefore be reportable to the ICO but not notifiable to an impacted individual. The research team agree with the shift to more realistic depictions of this scenario.

Accidental internal breach infographic: Scene 9

Pop up text: **“**Health services take many steps to support the security of your data. For example, services must review and report on their data security practices in line with clear regulatory standards, provide ongoing data security training to their staff, and appoint specific staff members who monitor and advise on data security to health services.

Click here to learn more about the safeguards in place by health services"

Visual: Return to the responsible health service characters from the introductory animation, featuring them again breaking down the roles/processes involved into individual people.

Lots of links: Participants and experts consulted suggested that there can be links from this text in the infographic to things like the DSPT and devolved nation equivalents, information about DPO roles, and training materials like the IT security videos for staff so that people have more specifics if they want it

Accidental internal breach infographic: Scene 10

Pop up text: “When it comes to the health service, the ICO have an array of tools to regulate how personal data is looked after. Their priority is to support services to make changes and prevent mistakes happening in the future. In the case of the most serious errors, organisations can receive large fines as a penalty for breaches*.

Repercussions Visual:
The participants suggested a judge-like figure representing the ICO sitting at a desk in an official-looking government type office, reviewing data security policies. There are legal documents and a scale of justice icon in the background.

Note: The experts consulted asked the ICO be depicted as an office worker not a judge, for accuracy. The wording has already been updated to make learning and support the focus, not fines, as they suggested.

However, it could be further considered to remove the wording about fines, *or add more text, e.g. '..but this is a last resort for the public sector as fines would take money out of the health service- hurting the patients.'