Infographic storyboard: Malicious External Breach

Co-developed 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

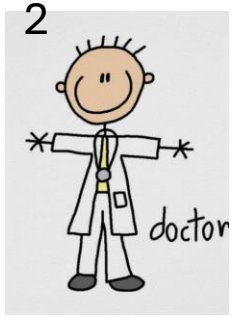
Summary of design decisions:

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

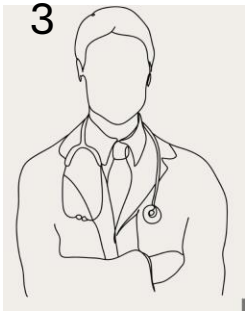
- **Tone:** Serious. It’s a serious issue, so not too playful. Realism- Not just a PowerPoint , properly moving through the story
- **Character design:** range of demographics to ensure relatable, 2D, no. 8. on real scale below, show emotions in expressions, all clearly different people. Healthcare workers 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 4: Malicious External Breach

Script and Storyboard

Malicious External breach : Scene 1

Pop up text:
“It’s the end of Rezina’s shift as a nurse in the intensive care unit.
Rezina sees an email urgently encouraging her to complete a security update by following a weblink.”

Visual: Rezina at the End of Her Shift

- Rezina, a nurse in her early 30s, wearing blue hospital scrubs, stands in front of her workstation in an intensive care unit. Her bag and coat are near showing she is preparing to leave. Rezina is depicted completely from behind, her dark coloured hair in a bun. We see Rezina’s work computer screen from over her shoulder, zoomed in, showing an email marked "URGENT: Profile/Security Update Required!" from what looks like a legitimate hospital administrator.
- **Background:** A hospital setting with medical monitors, patient beds, and dim evening lighting indicating the end of a shift.

Expert feedback: The wording was ‘update her hospital profile’ which feedback stated was a bit unclear . They didn’t know if it was the accepted phrase in hospitals. If not, ‘to complete a security update’ was thought to sound like a more likely phishing ploy. The research team agree.

Malicious External breach : Scene 2

Pop up text:
“Rezina clicks on the link, only to discover it was a scam email, designed to disrupt hospital services by blocking or stealing patient data on the IT system.

Visual: Rezina Clicks the Link

- Close-up of Rezina’s hand clicking on the email link with a concerned expression on her face. Screen flashing red, multiple pop ups, with warning signs like "ACCESS DENIED!" "DATA BREACH DETECTED!" and “SYSTEM LOCKED.”

Malicious External breach : Scene 3

Pop up text:
“This is a malicious external breach – patients' data has been purposely put at risk by an external force.”

Rezina later learns that many IT systems across the country have been badly affected by this cyberattack"

Visual: Hacker’s Perspective

- Split-screen effect—on one side, Rezina’s screen where her files have vanished; on the other, a hacker's screen where the same files appear. There may be some sort of energy flooding between. For the hacker, there is a dark room with a hooded hacker wearing a balaclava, typing rapidly, with lines of code streaming down their screen.
- To depict that the hacking may be across the country there could be arrows going to network of other hospitals, or Rezina's tableau multiplies across a map.

Malicious External breach : Scene 4

Pop up text:
“There are many different ways in which hackers might use these techniques to steal or corrupt patient data in the IT system. ”

Visual: setting the scene
Patient records dissolving/half disappearing.

Co-creation participants suggested the potential for an arrow starting to appear to point the direction to the first way/definition (phishing).

Malicious External breach : Scene 5

Pop up text: “One way is through a phishing' email. These are emails that trick an individual into revealing sensitive information, such as login credentials, which give the attacker access to internal IT systems.

"In a phishing attack, an attacker may steal the data and be able to view it or sell it on the black market which makes it very vulnerable."

Visual: Phishing Emails (Big text of the word 'Phishing'.)
Note: When depicting the external attacker co-creation participants had an appetite for dark, vivid imagery, with the sense of trying to test out the worst-case scenario. This urge is difficult to balance with the findings showing a desire for honesty and realism, and the expert guidance, which was that we don't know who these people are.

Suggestion 1: The participants suggested a visual of a scammer partially visible in a dimly lit, cluttered room. The hacker wears a black balaclava and a black-and-white striped top, sitting hunched over a desk littered with energy drink cans, junk food wrappers, and messy cables. Their hands hover over a keyboard. One hand moves forward to 'grab' digital files from the hospital system through the screen.

Suggestion 2: Showing it from Rezina's point of view. She has been tricked, she is devastated, she is reporting it immediately. Her screen is glitching- lines of code flash, and a faint lock symbol appears in the background.

Malicious External breach : Scene 6

Pop up text:
“Another is the use of scam emails which contain 'ransomware'. Opening a link in such email releases dangerous software onto the device, which encrypts the information on the device so that it cannot be accessed. Hackers may demand a ransom from the health service before the data can be accessed again.”

Visual: Ransomeware in Action

- The arrow now points to the other type: with a big 'Ransomeware' in text.
- Rezina again.

- Suggestion 1: Show a **padlock icon**, symbolizing encryption. The padlock bursts open, releasing **small digital "bugs" (malware insects)** that crawl into the computer.
- Suggestion 2: Simply make it clear that she can’t get into the patient information/it is gone, with files and folders disappearing from the screen, one by one, indicating data is being stolen.

- The hospital system’s dashboard fades to black, replaced by a flashing red warning: **“ACCESS DENIED.”**

Malicious External breach : Scene 7

Pop up text:
“In a ransomware attack, the attacker may not actually view or steal your data. However, the disruption can be huge both for hospitals who left unable to deliver care to its patients and for patients who are left unable to get care while feeling worried about this loss of privacy to their data.

Visual: The Impact on Hospitals

- A hospital waiting room with a long queue of anxious patients waiting to be seen. Some are checking their watches, looking frustrated, while others are visibly concerned about their medical information. Doctors and nurses rush around, stressed and confused.
- Signs on hospital equipment read **“OUT OF SERVICE”** and **“SERVICE DELAYED”** due to the ransomware attack.
- A receptionist at the front desk is on the phone, looking worried and overwhelmed.

Malicious External breach : Scene 8

Pop up “Even when quickly resolved, cyber attacks can leave serious consequences on the health and data of the public. This highlights why prevention is critical.

Visual: The lingering impact on Hospitals and next steps
Newspaper headlines, "Cancelled operations, appointments, long waits".

In the next scenes circle back to previous imagery regarding protections, be consistent with previous animation and infographics, reiterating the message of what the steps are and who is accountable.

Malicious External breach : Scene 9

Pop up

“The NHS takes extensive measures to prevent such occurrences.
However, if they occur, services must have plans in place to help them maintain services as best as possible. Where there is a likely high risk to patient data, they must also report the breach to the ICO and inform patients of the event within 72 hrs."

Visuals: Linking back to previous accountable health service characters, grouped together, clearly in an emergency response situation and taking their expected actions relevant to the text. Make sure the IT team is added. We're being moved through the structure of steps from the safety net.

Expert feedback: Not every cyber attack is a breach. In the case of systems going offline after cyber attack detection but back-up systems being quickly deployed, it may be the case that neither data confidentiality, nor availability, nor integrity of data is affected, and therefore no need to report to the ICO nor the data subjects. Suggestion for addition of "Where there is a likely high risk to patient data" to put the emphasis on reporting to ICO only where data subject rights and freedoms are impacted. Research team have made the suggested change.

Malicious External breach : Scene 10

Pop ups:

"The ICO will work with the affected organisations to learn from what went wrong and take steps to prevent it happening again."

“The ICO may take action, such as fines, against affected health services or the provider of the IT systems, if they find that security measures before the incident or the response to an incident falls short of what is needed to keep data safe

Visual: ICO imagery from previous animation/infographics. Ensure repetition to create the golden thread of consistent frameworks.

Note: Although expert stakeholders fed back that fines are a last result and uncommon in the public sector approach, they specified that they can be given to IT providers, and there are case studies on the ICO website of this e.g. Advance. Could have signpost here, "read more about the actions they have taken on their website".

Expert feedback: Suggestion for wording update: refer to incident not breach in the second sentence. This does seem to make sense if sometimes ‘the incident’ is not a breach.