January 2019

NHS Digital Data Security Centre – sector wide campaign toolkit

Design Brief

**Contents**

[1. Introduction to NHS Digital 3](#_Toc534641418)

[2. Introduction to NHS Digital’s Data Security Centre 3](#_Toc534641419)

[3. Background to the project 3](#_Toc534641420)

[4. Additional background information 4](#_Toc534641421)

[5. Project brief 4](#_Toc534641422)

[6. Production schedule 6](#_Toc534641423)

# Introduction to NHS Digital

* 1. NHS Digital is the national information and technology partner for the health and care system. We deliver and manage the digital infrastructure, services, products, data and standards upon which the health and care system in England depends. We are leading the delivery of the £4.2 billion National Information Board (“Paperless 2020”) agenda, which will transform the use of data and digital technologies by health and care organisations in England.

# Introduction to NHS Digital’s Data Security Centre

* 1. The NHS Digital Data Security Centre (DSC) supports increasingly digitised health and care organisations to manage cyber risk. This enables the safe and secure use of data and technology to deliver improved patient care. The DSC does this by providing a range of specialist services that help health and care organisations manage cyber risk and recover in the event of an incident.
	2. The DSC consists of a programme team delivering support services to health and care, the specialist security service overseeing security standards, policies and assurance, and a cyber security operations centre monitoring and alerting of internal and external threats.
	3. The DSC is not a regulator. Instead, it is an enabler, assisting (rather than policing) leaders and employees across the system to deliver better data security within their health and care organisations.

# Background to the project

* 1. Individual health and care organisations are accountable for their own cyber security, and all staff members have a role to play. By falling victim to cyber and security threats including phishing, password theft, tailgating and social engineering (see Annex 1 for further information), all staff across the NHS are potentially vulnerable to cyber/data security threats.
	2. The DSC has an objective to drive a cultural change throughout the health and care sector, increasing the perceived importance of and level of attention paid to data security. To do this, we need to educate all NHS staff on the direct impact of data security on patient care, and the steps they can take personally to reduce this impact/threat.
	3. The health and care sector in England is very broad, covering a myriad of organisations including trusts, GPs, pharmacists, opticians, dentists, social care providers and more. The NHS workforce alone is over 1.2 million people, and many of those employees lack knowledge about cyber and data security. In addition, there are often barriers to employees adopting the right behaviours e.g. time pressures. This poses a challenge, both in terms of how to reach as many of the workforce in acute trusts as possible, how to capture their attention, and how to leave them with some lasting practical knowledge and awareness of how to play their part in cyber/data security.
	4. There are many standard, routine activities that NHS staff perform on a daily basis in the interests of patient safety and care. These activities include handwashing and wearing minimal jewellery. Routine practices relating to cyber/data security should be equally habitual.
	5. Current deadline for project to be delivered is Friday 31 May 2019 but may be subject to change.

# Additional background information

* 1. Market research has been carried out with a variety of workforce groups in acute trusts (nurses, healthcare assistants, doctors and admin staff). This research has helped to benchmark the current levels of data and cyber security awareness/understanding. It should be used to inform the cyber campaign concept, messaging and design.
	2. A summary of this research is attached at Annex 2 to help inform proposals, the full results will be shared with the successful agency.
	3. An overview document detailing the different cyber and data security issues (phishing, password theft, tailgating and social engineering) that we wish to raise awareness of amongst staff is provided at Annex 1. The campaign should focus on making staff aware that cyber criminals use a range of tactics to trick staff rather than trying to embed the names of different types of attacks e.g. phishing or social engineering.

# Project brief

* 1. We would like to produce a toolkit of engaging communications materials that can be used by health and care organisations as an integrated staff-facing cyber/data security awareness campaign. We anticipate that organisations will run the campaign at different times of the year therefore it should be stand alone and work for any length of time or at any time of the year.
	2. By providing a ready-made toolkit of communications materials that can be tailored for use by NHS trusts and other health and care organisations (e.g. ability to add organisation’s logo), our aim is to empower them to run the campaign in a way that suits each organisation locally.
	3. The audience for this piece of work is the general health and care workforce, particularly those working for frontline organisations responsible for acute care (e.g. trusts). This audience is generally motivated by patient care and safety and uses a range of digital systems on a daily basis. It is possible that future iterations of this campaign may target other workforce groups e.g. pharmacists, GPs and social care. Therefore, consideration should be given to ensuring that creative ideas will flex for a secondary campaign phase.
	4. The campaign should:
		1. Raise awareness of the direct impact of cyber/data security on patient safety/care and help to embed a culture of cyber security throughout the NHS.
		2. Give NHS staff the knowledge and motivation to adopt basic cyber/data security practices (relating, for example, to phishing scams, passwords, tailgating and social engineering).
		3. Be clear and easy to understand by all staff groups (no previous knowledge of cyber security required and consideration should be given to staff with different accessibility needs).
		4. Ensure that staff understand that good data and cyber security enables patient care.
		5. Have an engaging, modern look and feel. It will need to stand out against other campaigns, information and day-to-day priorities and distractions, which are particularly prevalent in busy frontline locations such as hospitals.
		6. Be tested on NHS staff to ensure that the messages will be understood by a variety of workforce groups. Costs on the research or testing elements should be separately identifiable but included in the fixed cost tendered to deliver the campaign.
		7. Comply with and follow the NHS Digital brand guidelines (https://beta.nhsdigitalidentity.net/) and adopt the overall NHS identity (<https://www.england.nhs.uk/nhsidentity/>).
	5. The campaign should not adopt a sensationalist approach to cyber/data security as communications materials will be used in areas which are also shared with patients. However, highlighting the potential cyber risk from a simple every day task can create shock without being alarmist.
	6. We would envisage that the toolkit would be delivered in a digital format, and would include a combination of digital resources and printable digital files (which organisations could use to produce hard copy materials). Consideration should be given to organisations that may not have the budget to print large amounts of materials in colour.
	7. We would envisage that the campaign could have the potential for alignment with other high level national cyber security campaigns. This may involve work with other creative agencies to align the campaign materials.
	8. Communications materials we expect to be included within the toolkit are: flyers, posters, pop-up banners, web banners, web and social media graphics, screensavers/slideshows, email signatures, videos and case-studies/stories. This is not an exhaustive list, and we would expect our chosen supplier to help us develop the range of proposed materials and consider the context in which they will be seen.
	9. The campaign toolkit must:
		1. Be presented with a consistent and engaging look and feel, within the NHS brand guidelines and follow a campaign theme.
		2. Capture the attention of the audience, quickly communicate the core message that cyber/data security impacts patient care, and provide easily memorable/actionable guidance.
		3. Be easy to use by communications teams in health and care organisations, who may have differing levels of resource and expertise.
	10. The supplier will carry out the following work on the communications toolkit:
		1. Develop at least two outline campaign concepts, for presentation to NHS Digital (and associated stakeholders). NHS Digital will make the final concept choice.
		2. Provide expert guidance and suggestions as to format and delivery of a range of communications materials to be included in the toolkit.
		3. Design drafts of all materials for review, making amends as directed by NHS Digital (the agency should quote for a minimum of four rounds of amends).
		4. Prepare final versions of all toolkit materials and provide files in suitable formats for distribution.
		5. Provide copywriting and editorial support to NHS Digital’s communications team where appropriate.
		6. Benchmarking staff understanding ahead of the campaign launch and after the campaign has run, as well as overall campaign evaluation.
	11. The campaign should be delivered on a budget of less than £100,000.

# Production schedule

* 1. Key dates in the production schedule are given below but are subject to change:

|  |  |
| --- | --- |
| **Action** | **Date** |
| Issue Invitation to Tender | 17 January 2019 |
| Supplier Clarification Questions - Close  | 10am, 29 January 2019 |
| Supplier ITT submission closing date  | 10am, 4 February 2019 |
| Evaluation Stage 1 completed by evaluators | 7 February 2019 |
| Evaluator Moderation meeting | 8 February 2019 |
| Invite Suppliers to Present | 11 February 2019 |
| Supplier Presentations | 14 February 2019 |
| Evaluator Moderation meeting | 15 February 2019 |
| Intention to Award Letters issued  | 18 February 2019 |
| Standstill/ Alcatel Closes | Midnight 1 March 2019 |
| Contract commences | 4 March 2019 |
| First iteration of campaign materials provided for review | 29 March 2019 |
| NHS Digital to provide feedback on first iteration | 5 April 2019 |
| Deadline to deliver final campaign to NHS Digital | 31 May 2019 |