driving improvement and innovation in care

Adult Social Care Data and Cyber Security Programme 2019/20

Executive Summary

May 2020

Picture courtesy of Elizabeth Finn Homes

Adult Social Care Data and Cyber Security Programme 2019/20

Executive Summary

The adult social care sector is adopting technology to support care delivery. Whilst advances in technology bring benefits for the sector, and for the people the sector supports, they also present risks in how information is managed and kept secure.

To implement the outcomes of the National Cyber Security Strategy and identify the data and cyber security risks in the sector, Digital Social Care, the Local Government Association, NHS Digital and NHSX commissioned the Institute of Public Care at Oxford Brookes University (IPC) to deliver a discovery programme in 2018/19. The aim of the adult social care data and cyber security programme 2019/20 was to raise awareness of the importance of data and cyber security in the adult social care provider sector and to identify the extent to which recommendations in the 2018/19 programme report have been implemented.

Programme activity took place from July 2019 to the end of March 2020. Some activities at the end of the programme were curtailed due to the coronavirus crisis. The use of technology has changed rapidly since the lockdown. Not least that the Data Security and Protection Toolkit (DSPT) compliance requirements have been temporarily relaxed and a mass NHSmail onboarding process has begun. This report primarily reflects the activities and findings from the pre-pandemic situation. Nevertheless, the importance of data and cyber security has only increased as many digitally inexperienced care providers rapidly take up technology and criminals are using coronavirus to launch scams and cyber-attacks.

The programme supported 24 local projects and gave grants to 57 care providers, supporting many organisations to complete the DSPT as well as producing a wealth of data and cyber security guidance, training materials and other products. A key strength of the programme was the mix of organisations involved in the local projects - care providers, care associations, care provider representative bodies and councils – which allowed barriers and potential data and cyber security solutions to be explored from different perspectives.

A key conclusion of the programme is that the toolkit continues to be a “hard sell” for regulated providers and is little known by other organisations in the sector. Barriers to its use at scale include the registration process and complexity of the toolkit’s headquarters functionality, an NHS focus, and off-putting language and jargon. Most small and medium sized social care organisations will struggle to complete the DSPT in any meaningful way without support and guidance. We recommend that a social care specific assessment is developed with questions that are written in plain English so that they are more easily understood.

There are real benefits to be had from moving on-line in the 'right way' and making best use of the available technology. However, the data and cyber security issues and concerns that were identified in the 2018/19 programme are still very much present and there is little evidence to suggest that general risk levels across the sector have reduced over the last year. Key risks for the sector continue to be safe use of smartphones, passwords, backups and staff training and awareness raising. In addition, publication of the toolkit does not necessarily prompt social care providers to take comprehensive cyber security measures.

The use of personal digital devices for work purposes is common across the sector, but many providers remain unaware of the risks of staff using their own devices. We advise all providers think about the implications of this and develop bring your own device (BYOD) policies and implement better security measures such as some form of mobile device management.

Digital literacy of staff in the sector is low. Making this part of the job role with an expectation of basic IT skills for all care staff is a crucial next step for the sector. Future programme support should recognise that there are a significant number of providers who struggle with even basic IT and that issues of patchy internet connectivity and digital infrastructure need to be addressed.

Culture change and skills development related to technology can be a challenge for the workforce, but digital champions and good training can make a difference. Improving the digital literacy of staff must include better awareness of data and cyber security for all types of roles working in the sector. We found that, whilst there is a wide range of data and cyber security training materials available for use (some free and some at a cost), there is nothing specifically targeted at the social care sector. Developing and promoting better, social care specific awareness raising and training materials is a priority.

We encourage councils and health commissioners to support local care providers with data and cyber security. We developed guidance that makes suggestions as to how commissioners of adult social care might support providers to adopt appropriate safeguards. This includes the recommendation that commissioners consider building into contracts with providers the requirement to complete the DSPT.

The introduction of Digital Social Care since the 2018/19 programme is a welcome development. The social care specific resources and support available from the website were well thought of and valued by all involved in the programme. However, there is low awareness of the website across the sector and we recommend that it is promoted more widely. Digital Social Care has set up a helpline to support the adult social care sector with harnessing technology during the coronavirus crisis. This, it seems to us, is a model that could be replicated to support the sector to complete the DSPT, use NHSmail or other digital tools, and improve data and cyber security post-pandemic.