Department of Health & Social Care

Sarah Wilkinson
Chief Executive
NHS Digital
1 Trevelyan Square
Boar Lane
Leeds
LS1 6AE

Date

Dear Sarah,

Data Security and Protection Incident Reporting Tool Direction 2018

I am writing to provide a Direction to the Health and Social Care Information Centre, known as, and hereafter referred to in this Direction as NHS Digital.

This Direction is given in exercise of the powers conferred by sections 254(1) and (6) and 260(1) and (2)(d) of the Health and Social Care Act 2012 (**the Act**) and 304(9), (10) and (12) of the Health and Social Care Act 2012 (**the Act**) and Regulation 32 of the National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013 (**the Regulations**).

This Direction is to be known as the '**Data Security and Protection Incident Reporting Tool Direction 2018**' and comes in to force on 24 May 2018. In exercising the functions described in this Direction, NHS Digital must have regard to such priorities, policies, advice or guidance of the Secretary of State for Health and Social Care as the Secretary of State may notify in writing from time to time to NHS Digital.

Pursuant to sections 254(1) and 254(6) of the Act, NHS Digital is directed to receive electronic information from health and social care organisations about their data security incidents and notify the relevant regulators and Arm's-Length Bodies to support compliance with the General Data Protection Regulation (**GDPR**) and the

Network and Information Systems Regulations 2018 (**NIS Regulations**) in accordance with section 261(3) of the Act.

The NIS Regulations came into force on 10 May 2018, and require providers of essential healthcare services defined therein to notify the Secretary of State, as the designated competent authority, about any incident which has a significant impact on the continuity of the essential service which they provide.

The GDPR comes into force on 25 May 2018 and places a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority which is the Information Commissioner in the United Kingdom.

The information to be collected is set out in Annex A, which may be reviewed from time to time.

In accordance with section 260(2)(d) of the Act, NHS Digital is directed not to publish details of specific incidents including details of which organisations were involved in these incidents. Summary and aggregate information about trends in incidents across the health and social care sector will be routinely published by NHS Digital after a period of collection and analysis, in accordance with section 260(1) of the Act.

In accordance with section 254(2)(b) of the Act, the Secretary of State considers that it is in the interests of the health service in England or of the recipients or providers of adult social care in England for this Direction to be given.

In accordance with section 254(5) of the Act, NHS Digital has been consulted before this Direction has been given.

Yours sincerely

Iain O'Neil
Deputy Director of Digital and Technology Strategy

Annex A

Details of the information being collected due to the **Data Security and Protection Incident Reporting Tool Direction 2018** and the organisations with which this information will be shared.

ID	Information Requested	Notification Purpose	Organisation with which information is to be shared if criteria met
1	Organisation Name	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
2	Organisation Code	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
3	Name of the person Submitting incident	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
4	Email Address of person Submitting incident	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
5	Sector	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
6	What has happened?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
7	How did you find out?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
8	Was the incident caused by a problem with a network or an information system?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
9	What is the local ID for this incident?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
10	When did the incident start?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
11	Is the incident still on going?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
12	Have data subjects or users been informed?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
13	Is it likely that citizens outside England will be affected?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
14	Have you notified any other (overseas) authorities about this incident?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
15	Have you informed the Police?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
16	Have you informed any other regulatory bodies about this incident?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
17	Has there been any media coverage of the incident (that you are aware of)?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital

18	What other actions have been taken or are planned?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
19	How many people are affected?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
20	Who is affected?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
21	What is the likelihood that people's rights have been affected?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
22	What is the severity of the adverse effect?	GDPR and NIS	ICO, DHSC, NCSC and NHS Digital
23	Has there been any potential clinical harm as a result of the incident?	NIS	ICO, DHSC, NCSC and NHS Digital
24	Has the incident disrupted the delivery of healthcare services?	NIS	ICO, DHSC, NCSC and NHS Digital
25	Which of these services are operated by your organisation?	NIS	ICO, DHSC, NCSC and NHS Digital