Department of Health & Social Care

NHS England

Classification: Official

To: • CEOs of suppliers to the NHS

NHS England
Wellington House
133-155 Waterloo Road
London
SE1 8UG

15 May 2025

DRAFT

Dear all,

For action: Sign the Cyber Security Charter

This is an open letter to all current, potential or aspiring suppliers to the NHS, to highlight the growing and ever-changing cyber security threat level that we collectively face. The severity of incidents, and increasing frequency, has demonstrated a step change in recent months.

Ransomware, a type of malware which prevents you from accessing your devices and the data stored on it, usually by encrypting your files, is endemic and we have experienced several significant ransomware attacks on our supply chain in recent years.

The Cyber Security and Resilience Bill aims to expand the remit of cyber regulation, including the Network and Information Systems (NIS) Regulations, to protect more digital services and supply chains against the growing threat.

As valued partners to the NHS, it is important to us that we work together and defend as one. We are therefore asking you to ensure where reasonably necessary, for example, if your service to an NHS organisation supports clinical systems or involves processing (including storage) of confidential information including confidential patient information that:

- Your systems are kept in support and have the latest patches applied to address known vulnerabilities.
- You will achieve and maintain at least “Standards Met” as part of the Data Security and Protection Toolkit (DSPT).
- You will apply Multi-Factor Authentication (MFA) to your own networks and systems. In order to support our customers to meet the NHSE MFA Policy, you will support

identity federation or make MFA functionality available on the products that you provide.

- You will deploy effective 24/7 cyber monitoring and logging of your critical IT infrastructure to prevent and detect cyber-attacks, which will allow investigation in the event of an incident.

- You will ensure that you have immutable backups of your critical business data, with tested plans that ensure you can offer business continuity and rapid recovery of essential IT. You will also have immutable backups of your products to ensure the continued provision of the systems and services that you provide.

- You have undertaken board level exercising to ensure you are confident of your ability to respond in the event of a cyber-attack.

- You will report to your clients in a timely manner, adhering to all regulatory requirements, and work collaboratively, openly and in partnership with NHS England in the event of discovering a cyber-attack affecting patient care or data.

- Where providing software to the NHS you will agree that the software has been produced in adherence to the DSIT/NCSC Software Code of Practice and commit to meeting the principles of secure design and development, secure build environment, secure deployment and maintenance and communication with customers.

What you need to do

1. Commit to being an outstanding and trusted partner to the NHS, by signing up to our public charter on cyber security good practice. This voluntary charter will contain the asks outlined above and show your commitment to being a trusted and secure partner to the health and care system. We will be launching a self-assessment form in the Autum, whereby suppliers can sign the charter. This will allow time for suppliers to work through the eight statements and be ready to commit.

2. Join us in future supplier summits and engagement opportunities to understand how we can collaborate on keeping the NHS safe from and resilient to attack.

3. Work with your local NHS customer to mutually improve your understanding and preparation for an incident.

Ongoing obligations and arrangements

In addition to the voluntary commitment that you make to signing up to the Cyber Security Charter, your organisation will also have legal obligations to maintain the cyber security of the processes and systems you operate under arrangements with NHS organisations. These include the contractual terms with such NHS organisations as well as the statutory obligations including (but not limited to) Article 32 of UK GDPR to have in place appropriate

DRAFT

Copyright © NHS England 2025

technical and organisational measures to ensure a level of security appropriate to the risks to personal data.

- Signing up to the Cyber Security Charter is a helpful and positive step, but it does not amount to a legal obligation and does not result in priority or enhanced status in terms of the tendering process for contracts with NHS organisations.

- The requirements of the DSPT remain whether or not you sign-up to the Cyber Security Charter.

Further support

We recognise that continuous improvements in cyber resilience in the face of increasing and changing threat is a significant challenge and we are taking steps to play our part nationally through the following:

- We are developing tools that providers can use to identify their critical suppliers to carry out appropriate assurance.
- We are defining requirements for a national supplier management platform to help us map the supply chain, alongside developing a risk assurance model allowing us to identify and mitigate concentration risk.
- We are reviewing the contractual frameworks that NHS organisations use to enter contracts, so they have the appropriate security schedules and expectations are clear. This is part of a cross-government initiative to review contractual cyber security schedules and clauses.

We are here to support our suppliers every step of the way and will be launching a series of webinars over the coming months and building a supplier forum for cyber security in the Autumn. In the meantime, please contact england.cyber@nhs.net for any queries.

We are grateful for your support on this important issue.

Yours sincerely

Vin Diwakar,	**Phil Huggins**	**Mike Fell**
National Director of Transformation	National Chief Information Security Officer for Health and Care	Director of Cyber Operations
NHS England	Department of Health and Social Care	NHS England

DRAFT

Copyright © NHS England 2025