NHS in England hit by 'cyber-attack'

12/05/2017

The National Health Service has been hit by a large cyber attack, with hospitals across England reporting that their IT systems are down.

NHS Digital, the arm of the health service co-ordinating a response, said it was “aware an incident had taken place and steps are being taken to resolve that incident”.

Several hospitals had been affected, it added, but it did not yet know how many. Nor was it able to confirm how the incident had affected patients.

The same or a similar virus also appears to have been used in a large-scale attack in Spain on Friday that hit companies including Telefónica, the country’s main telecoms provider. Telefónica said it had suffered a “cyber security incident” affecting the personal computers of “some” employees.

It is not known if the attacks in Spain and on England’s NHS are connected. There have been more unverified reports of cyber attacks in several other countries.

The hackers are thought to have deployed a virulent version of ransomware known as WannaCry. Typically, hackers will seek to infect IT systems with ransomware in order to demand money to “unlock” the affected computers.

Barts Hospital, in central London, confirmed it was among the hospitals to have been hit and said it had been forced to cancel routine appointments and divert ambulances to neighbouring

hospitals as the “major IT disruption” took hold. It asked the public “to use other NHS services wherever possible” and said the IT breakdown was causing delays at all the hospitals within the trust.

“We have activated our major incident plan to make sure we can maintain the safety and welfare of patients,” it added. The switchboard had been affected at Newham Hospital in east London but direct-line phones were still working.

East and North Hertfordshire NHS Trust was also hit. It posted a statement on its website to say it was “currently experiencing significant problems with our IT and telephone network which we’re trying to resolve as soon as possible”.

Hospital trusts and GP groups in Lancashire were also reporting problems.

Vanessa Sandhu, a GP in Braintree, said: “We got a call from the CCG [Clinical Commissioning Groups] saying there had been a security breach. We all had to shut down our computers and unplug all cables from the walls.

“It was scary — we had no idea what was going on. We didn’t have access to our notes or patient medical records. We couldn’t request blood tests or ultrasounds. We had to disconnect the surgery telephones so we couldn’t communicate with other doctors or patients. We tried to see the patients in the building, but everyone else we told to go home.

“We’ve had to close the surgery for the day. Some hospitals have had to shut down so it’s going to be absolute carnage in A&E if you can’t do emergency tests or get blood results for those most in need.”

In February a report into the NHS and cyber crime found that 34 per cent of trusts across England, Scotland and Wales had suffered ransomware attacks during the previous 18 months. Scottish trusts were the worst hit, with almost 60 per cent being attacked, while 79 English trusts, more than 33 per cent, had been affected since June 2015.

Attacks on at least seven of the trusts, including dozens of hospitals, had been successful, which means data had been locked up by criminals.

In November a ransomware attack on the Northern Lincolnshire and Goole Trust brought down the systems of three British hospitals, forcing doctors to use pen and paper rather than computers, and leading to the cancellation of hundreds of routine operations and outpatient appointments. The attack lasted five days.

Paul Flynn, a Labour MP, told the Financial Times that Friday’s attack was “absolutely terrifying” and argued that the government was woefully unprepared for such incidents.

“We are blundering around in the dark, we are trying to defend our institutions with systems that are right out of the 19th century,” he said. “We are so vulnerable to this kind of thing — it is alarming that they can get through the system so easily. There must be lives that are under threat.”

Jonathan Ashworth, shadow health secretary, said the attack was “a real worry for patients” and called on the government to set out what had happened and what measures ministers were taking to reduce the threat.

“This incident highlights the risk to data security within the modern health service and reinforces the need for cyber security to be at the heart of government planning. The digital revolution has transformed the way we live and work but we have to be ready for the vulnerabilities it brings too,” he said.

“The safety of the public must be the priority and the NHS should be given every resource to bring the situation under control as soon as possible.”