National Audit Office

Report
by the Comptroller
and Auditor General

Department of Health

Investigation: WannaCry cyber attack and the NHS

HC 414 SESSION 2017–2019 27 OCTOBER 2017

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of £734 million in 2016.

National Audit Office

Department of Health

Investigation: WannaCry cyber attack and the NHS

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 25 October 2017

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Sir Amyas Morse KCB
Comptroller and Auditor General
National Audit Office

24 October 2017

HC 414 | £10.00

This report investigates the NHS's response to the cyber attack that affected it in May 2017 and the impact on health services.

Investigations

We conduct investigations to establish the underlying facts in circumstances where concerns have been raised with us, or in response to intelligence that we have gathered through our wider work.

11594 10/17 NAO

Contents

The National Audit Office study team consisted of:
Finnian Bamber, Alex Bowyer, Nigel Leung, Francisca Lopes, Linda Mills and David Williams, under the direction of Robert White.

This report can be found on the National Audit Office website at www.nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

What this investigation is about

1 On Friday 12 May 2017 a global ransomware attack, known as WannaCry, affected more than 200,000 computers in at least 100 countries. In the UK, the attack particularly affected the NHS, although it was not the specific target. At 4 pm on 12 May, NHS England declared the cyber attack a major incident and implemented its emergency arrangements to maintain health and patient care. On the evening of 12 May a cyber-security researcher activated a kill-switch so that WannaCry stopped locking devices.

2 According to NHS England, the WannaCry ransomware affected at least 81 out of the 236 trusts across England, because they were either infected by the ransomware or turned off their devices or systems as a precaution. A further 603 primary care and other NHS organisations were also infected, including 595 GP practices.

3 Before the WannaCry attack the Department of Health (the Department) and its arm's-length bodies had work under way to strengthen cyber-security in the NHS. For example, NHS Digital was broadcasting alerts about cyber threats, providing a hotline for dealing with incidents, sharing best practice and carrying out on-site assessments to help protect against future cyber attacks; and NHS England had embedded the 10 Data Security Standards (recommended by the National Data Guardian) in the standard NHS contract for 2017-18 and was providing training to its Board and local teams to raise awareness of cyber threats. In light of the WannaCry attack, the Department announced further plans to strengthen NHS organisations' cyber-security.

4 Our investigation focuses on events immediately before 12 May 2017 and up until 30 September 2017. We only cover the effect the WannaCry attack had on the NHS in England. We do not cover how the WannaCry attack affected other countries or organisations outside the NHS. A cyber attack on either the health or social care sectors could cause disruption across the whole health and social care sector. For example, the Care Quality Commission (CQC) told us that, as some trusts were unable to communicate with social services, there could have been delays in the discharge of patients from hospital to social care, although the CQC relayed advice from NHS Digital and NHS England to social care providers to help manage any disruption. This investigation sets out the facts about:

- the ransomware attack's impact on the NHS and its patients;
- why some parts of the NHS were affected; and
- how the Department and NHS national bodies responded to the attack.

Summary

1 The WannaCry attack affected NHS services in the week from 12 May to 19 May 2017. The Department of Health (the Department) and NHS England worked with NHS Digital, NHS Improvement, the National Cyber Security Centre, the National Crime Agency and others to respond to the attack.

Key findings

The risk of a cyber attack affecting the NHS

2 WannaCry was the largest cyber attack to affect the NHS, although individual trusts had been attacked before 12 May 2017. For example, two of the trusts infected by WannaCry had been infected by previous cyber attacks. One of England's biggest trusts, Barts Health NHS Trust, had been infected before, and Northern Lincolnshire and Goole NHS Foundation Trust had been subject to a ransomware attack in October 2016, leading to the cancellation of 2,800 appointments (paragraph 3.7 and Figure 5).

3 The Department was warned about the risks of cyber attacks on the NHS a year before WannaCry and although it had work under way it did not formally respond with a written report until July 2017. The Secretary of State for Health asked the National Data Guardian and the Care Quality Commission (CQC) to undertake reviews of data security. These reports were published in July 2016 and warned the Department that cyber attacks could lead to patient information being lost or compromised and jeopardise access to critical patient record systems. They recommended that all health and care organisations needed to provide evidence that they were taking action to improve cyber-security, including moving off old operating systems. Although the Department and its arm's-length bodies had work under way to improve cyber-security in the NHS, the Department did not publish its formal response to the recommendations until July 2017 (paragraphs 3.6 and 3.11).

4 The Department and its arm's-length bodies did not know whether local NHS organisations were prepared for a cyber attack. Local healthcare organisations such as trusts and clinical commissioning groups are responsible for keeping the information they hold secure, and for having arrangements in place to respond to an incident or emergency, including a cyber attack. Local healthcare bodies are overseen by the Department and its arm's-length bodies. The Department and Cabinet Office wrote to trusts in 2014, saying it was essential they had "robust plans" to migrate away from old software, such as Windows XP, by April 2015. In March and April 2017, NHS Digital had issued critical alerts warning organisations to patch their systems to prevent WannaCry. However, before 12 May 2017, the Department had no formal mechanism for assessing whether NHS organisations had complied with its advice and guidance. Prior to the attack, NHS Digital had conducted an on-site cyber-security assessment for 88 out of 236 trusts, and none had passed. However, NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of an organisation (paragraphs 2.5, 2.7, 2.10 to 2.12 and 3.2, and Figure 4).

How the WannaCry attack affected the NHS

5 The attack led to disruption in at least 34% of trusts in England although the Department and NHS England do not know the full extent of the disruption (Figure 1). On 12 May, NHS England initially identified 45 NHS organisations including 37 trusts that had been infected by the WannaCry ransomware. Over the following days, more organisations reported they had been affected. In total, at least 81 out of 236 trusts across England were affected. The trusts included:

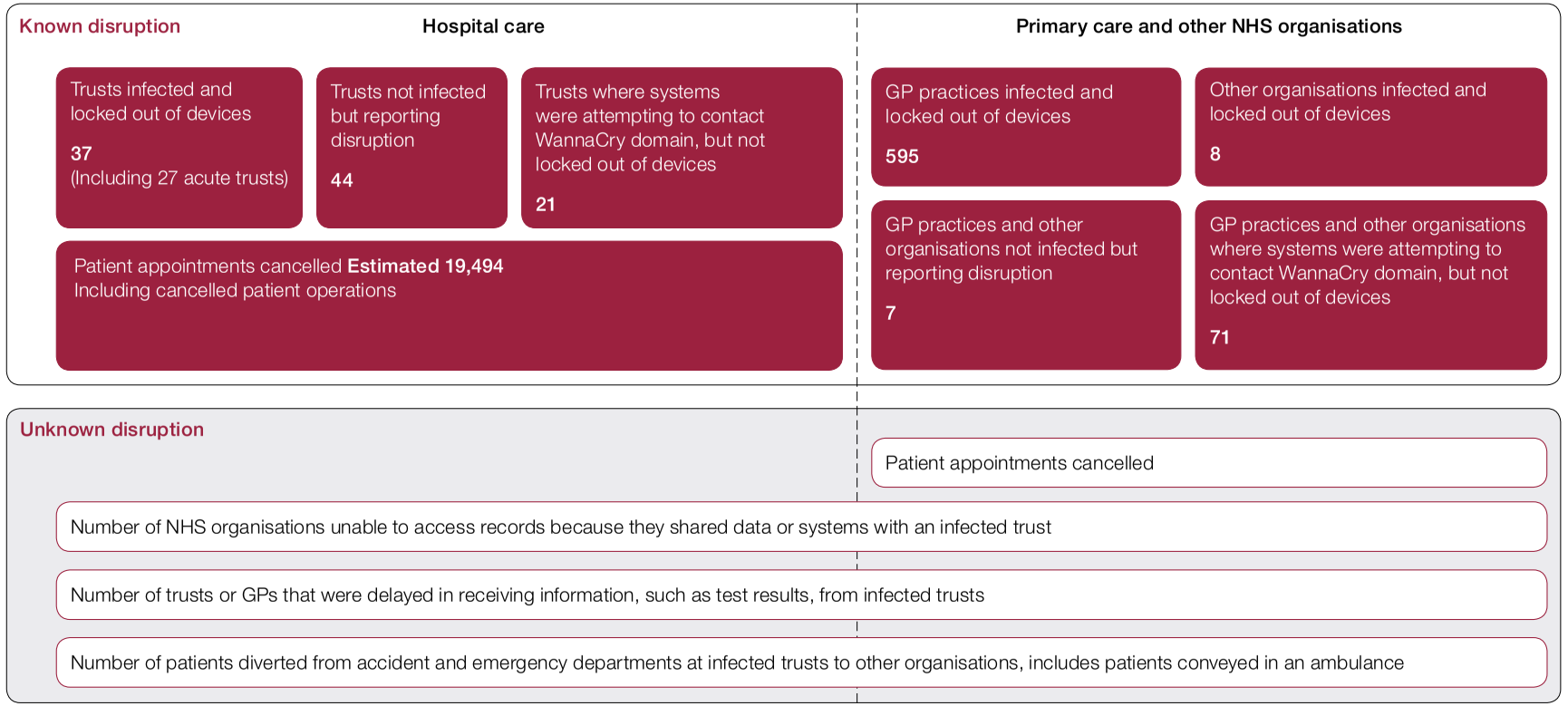
- 37 infected and locked out of devices (of which, 27 were acute trusts); and
- 44 not infected but reporting disruption. For example, these trusts shut down their email and other systems as a precaution and on their own initiative, as they had not received central advice early enough on 12 May to inform their decisions on what to do. This meant, for example, that they had to use pen and paper for activities usually performed electronically.

NHS England and NHS Digital identified a further 21 trusts that were attempting to contact the WannaCry domain, but were not locked out of their devices. There are two possible reasons for this. Trusts may have become infected after the kill-switch had been activated, and were therefore not locked out of their devices. Alternatively, they may have contacted the WannaCry domain as part of their cyber-security activity.

A further 603 primary care and other NHS organisations were infected by WannaCry, including 595 GP practices. However, the Department does not know how many NHS organisations could not access records or receive information, because they shared data or systems with an infected trust. NHS Digital told us that it believes no patient data were compromised or stolen (paragraphs 1.2 to 1.5 and 1.9, and Figure 1).

Figure 1
The impact of WannaCry on the NHS

The NHS experienced a wide range of disruption as a consequence of the WannaCry cyber attack



Notes

1 'Other organisations' include clinical commissioning groups, commissioning support units, an NHS 111 provider, and non-NHS bodies that provide NHS care, such as a hospice, social enterprise and community interest companies.

2 The numbers shown are based on organisations self-reporting problems to national bodies, and NHS England and NHS Digital's analysis of internet activity, and may be higher if some organisations did not report the problems they experienced in a timely or accurate way.

3 Some of the trusts identified as not infected but reporting disruption did have a small number of devices infected. However, they did not report themselves to NHS England as infected, and NHS England did not recategorise them as being infected after the WannaCry attack was over.

4 Some trusts, GP practices and other organisations were identified as having systems that attempted to contact the WannaCry domain, but were not locked out of their devices. There are two possible explanations for this: they could have become infected after the kill-switch had been activated. Or, they could have avoided infection but contacted the WannaCry domain as part of their cyber-security activity. NHS England does not know which organisations fall into each category.

Source: National Audit Office analysis of NHS England data

6 **Thousands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments.** Between 12 May and 18 May, NHS England collected some information on cancelled appointments, to help it manage the incident, but this did not include all types of appointment. NHS England identified 6,912 appointments had been cancelled, and estimated more than 19,000 appointments would have been cancelled in total, based on the normal rate of follow-up appointments to first appointments. NHS England told us it does not plan to identify the actual number because it is focusing its efforts on responding appropriately to the lessons learned from WannaCry. As data were not collected during the incident, neither the Department nor NHS England know how many GP appointments were cancelled, or how many ambulances and patients were diverted from the five accident and emergency departments that were unable to treat some patients (paragraphs 1.7, 1.8 and 1.10, and Figure 1).

7 **The Department, NHS England and the National Crime Agency told us that no NHS organisation paid the ransom, but the Department does not know how much the disruption to services cost the NHS.** The Department, NHS England and the National Crime Agency told us no NHS organisation paid the ransom. NHS Digital told us it advised the trusts it spoke to not to pay the ransom, and wrote to all trusts on 14 May advising against the payment of ransoms. The Department does not know the cost of the disruption to services. Costs include: cancelled appointments; additional IT support provided by local NHS bodies, or IT consultants; or the cost of restoring data and systems affected by the attack. National and local NHS staff worked overtime including over the weekend of 13-14 May to resolve problems and to prevent a fresh wave of organisations being affected by WannaCry on Monday 15 May (paragraphs 1.11 and 1.12).

8 **The cyber attack could have caused more disruption if it had not been stopped by a cyber researcher activating a 'kill-switch'.** On the evening of 12 May a cyber-security researcher activated a 'kill-switch' so that WannaCry stopped locking devices. This meant that some NHS organisations had been infected by the WannaCry ransomware, but because of the researcher's actions, they were not locked out of their devices and systems. Between 15 May and mid-September NHS Digital and NHS England identified a further 92 organisations, including 21 trusts, as contacting the WannaCry domain, although some of these may have been contacting the domain as part of their cyber-security activity. Of the 37 trusts infected and locked out of devices, 32 were located in the North NHS region and the Midlands and East NHS region. NHS England believes more organisations were infected in these regions because they were hit early on 12 May before the WannaCry 'kill-switch' was activated (paragraphs 1.14 and 2.2, and Figure 3).

The NHS response to the attack

9 **The Department had developed a plan, which included roles and responsibilities of national and local organisations for responding to an attack, but had not tested the plan at a local level.** This meant the NHS was not clear what actions it should take when affected by WannaCry. NHS England found that responding to WannaCry was different from dealing with other incidents, such as a major transport accident. Because WannaCry was different it took more time to determine the cause of the problem, the scale of the problem and the number of organisations and people affected (paragraph 3.3 and Figure 2).

10 **As the NHS had not rehearsed for a national cyber attack it was not immediately clear who should lead the response and there were problems with communications.** The WannaCry attack began on the morning of 12 May. At 4 pm NHS England declared the cyber attack a major incident and at 6:45 pm initiated its existing Emergency, Preparedness, Resilience and Response plans to act as the single point of coordination for incident management, with support from NHS Digital and NHS Improvement. In the absence of clear guidelines on responding to a national cyber attack, local organisations reported the attack to different organisations within and outside the health sector, including local police. Communication was difficult in the early stages of the attack as many local organisations could not communicate with national NHS bodies by email as they had been infected by WannaCry or had shut down their email systems as a precaution, although NHS Improvement did communicate with trusts' chief executive officers by telephone. Locally, NHS staff shared information through personal mobile devices, including using the encrypted WhatsApp application. Although not an official communication channel, national bodies and trusts told us it worked well during this incident (paragraphs 3.3 to 3.5 and Figure 2).

11 **In line with its existing procedures for managing a major incident, NHS England initially focused on maintaining emergency care.** Since the attack occurred on a Friday this caused minimal disruption to primary care services, which tend to be closed over the weekend. Twenty-two of the 27 infected acute trusts managed to continue treating urgent and emergency patients throughout the weekend. However, five – in London, Essex, Hertfordshire, Hampshire and Cumbria – had to divert patients to other accident and emergency departments, and a further two needed outside help to continue treating patients. By 16 May only two hospitals were still diverting patients. The recovery was helped by the work of the cyber-security researcher that stopped WannaCry spreading (paragraphs 1.7, 1.13 and 1.14).

Lessons learned

12 NHS Digital told us that all organisations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves. All NHS organisations infected by WannaCry had unpatched or unsupported Windows operating systems so were susceptible to the ransomware. However, whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded organisations against infection. NHS Digital told us that the majority of NHS devices infected were unpatched but on supported Microsoft Windows 7 operating systems. Unsupported devices (those on XP) were in the minority of identified issues. NHS Digital has also confirmed that the ransomware spread via the internet, including through the N3 network (the broadband network connecting all NHS sites in England), but that there were no instances of the ransomware spreading via NHSmail (the NHS email system) (paragraphs 1.2, 1.6 and 2.4 to 2.6).

13 There was no clear relationship between vulnerability to the WannaCry attack and leadership in trusts. We found no clear relationship between trusts infected by WannaCry and the quality of their leadership, as rated by the Care Quality Commission (paragraph 2.8).

14 The NHS has accepted that there are lessons to learn from WannaCry and is taking action. Lessons identified by the Department and NHS national bodies include the need to:

- develop a response plan setting out what the NHS should do in the event of a cyber attack and establish the roles and responsibilities of local and national NHS bodies and the Department;
- ensure organisations implement critical CareCERT alerts (emails sent by NHS Digital providing information or requiring action), including applying software patches and keeping anti-virus software up to date;
- ensure essential communications are getting through during an attack when systems are down; and
- ensure that organisations, boards and their staff are taking the cyber threat seriously, understand the direct risks to front-line services and are working proactively to maximise their resilience and minimise impacts on patient care.

Since WannaCry, NHS England and NHS Improvement have written to every trust, clinical commissioning group and commissioning support unit asking boards to ensure that they have implemented all 39 CareCERT alerts issued by NHS Digital between March and May 2017 and taken essential action to secure local firewalls (paragraphs 3.8 and 3.9).

Part One

The impact of the cyber attack

1.1 WannaCry was the largest ever cyber attack to affect the NHS in England. The timeline of the main events relating to the WannaCry ransomware attack which affected NHS services in the week from 12 May to 19 May 2017 is set out in **Figure 2** overleaf.

The scale of the attack

1.2 NHS Digital told us that the ransomware spread via the internet, including through the N3 network. As shown in Figure 1 (page 7), the WannaCry ransomware attack affected at least 81 out of 236 trusts across England. These numbers are based on NHS organisations' own reports to NHS England. Of these 81 trusts, there were:

- 37 trusts infected and locked out of devices (of which, 27 were acute trusts); and
- 44 trusts not infected but reporting disruption.

NHS England and NHS Digital identified a further 21 trusts that were attempting to contact the WannaCry domain, but were not locked out of their devices. There are two possible reasons for this. Trusts may have become infected after the kill-switch had been activated, and were therefore not locked out of their devices.[1] Alternatively, they may have contacted the WannaCry domain as part of their cyber-security activity.

1.3 The trusts infected by the WannaCry ransomware experienced two main types of disruption including:

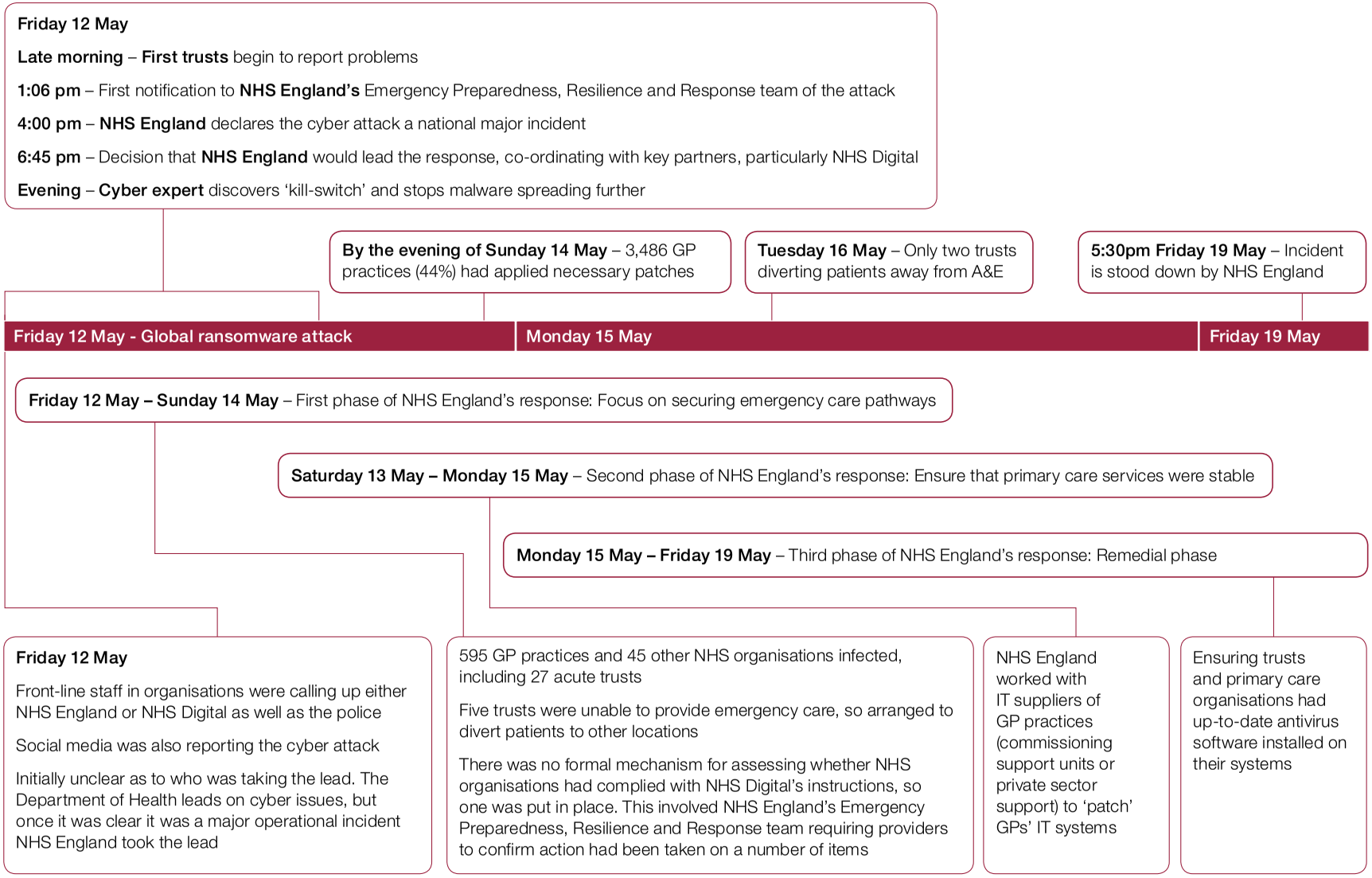
- NHS staff being locked out of devices, which prevented or delayed staff accessing and updating patient information, sending test results to patients' GPs and transferring or discharging patients from hospital; and
- medical equipment and devices being locked, or isolated from trusts' IT systems to prevent them being locked. This meant trusts' radiology and pathology departments were disrupted as the trusts relied on the equipment and devices for diagnostic imaging (such as MRI scanners) and for testing blood and tissue samples.

1 A 'kill-switch' is a mechanism that is incorporated into software to shut down that software, or the device on which it sits, in an emergency situation in which it cannot be shut down in the usual manner.

Figure 2

Timeline of the WannaCry attack from 12 May to 19 May 2017

NHS England emergency response to WannaCry lasted one week



Source: National Audit Office

As at 19 May 2017, NHS England had identified 1,220 pieces of diagnostic equipment that had been infected, 1% of all such NHS equipment. Although a relatively small proportion of devices, the figure does not include devices disconnected from IT systems to prevent infection. The trusts we spoke to told us about the disruption they had experienced due to diagnostic equipment being infected or isolated, such as not being able to send MRI scan results to clinicians treating patients in other parts of the hospital.

1.4 The disruption at trusts not infected by the ransomware was caused by:

- the absence of timely central direction, leading to the trusts taking actions on their own initiative to avoid becoming infected, including shutting down devices or isolating devices from their networks to protect themselves from the ransomware; or
- trusts not being able to access electronic patient records or receive information, such as test results, because they shared data or systems with an infected trust which had shut down its systems; or
- trusts disconnecting from the N3 network, the broadband network connecting all NHS sites in England.

1.5 The disruption at these trusts took a number of forms. For example, some trusts had to use manual workarounds to perform their usual tasks, such as providing medication to patients, and record information using pen and paper. In addition, organisations could not receive external emails, so communication with national bodies and others outside their trust was severely limited.

1.6 Despite widespread local disruption, NHS Digital told us that national NHS IT systems managed by NHS Digital were not infected, such as the NHS Spine (a service holding secure databases of demographic and clinical information) and NHSmail (the NHS email system).

1.7 Of the 27 acute trusts infected and locked out of devices, five had to divert emergency ambulance services to other hospitals. The five trusts and hospitals were:

- Barts Health NHS Trust (Royal London Hospital);
- Mid Essex Hospital Services NHS Trust (Broomfield Hospital);
- East and North Hertfordshire NHS Trust (Lister Hospital);
- Hampshire Hospitals NHS Foundation Trust (Basingstoke Hospital); and
- North Cumbria University Hospitals NHS Trust (West Cumberland Hospital).

The impact on patients

1.8 As infected NHS organisations could not access important information and electronic systems, including patient records, they had to cancel appointments and operations and some trusts had to divert patients to other accident and emergency departments. Between 12 May and 18 May, NHS England collected some information on how many appointments had been cancelled to help it manage the incident, but did not collect data on all types of appointment. NHS England identified that the NHS had cancelled 6,912 appointments, but this figure does not include repeat outpatient appointments and cancellations identified after 18 May. NHS England estimated the total number of cancelled appointments as being around 19,494, based on the normal rate of follow-up appointments to first appointments, but told us it does not plan to identify the actual number because it is focusing its efforts on responding appropriately to the lessons learned from WannaCry. NHS England did not collect data on how many GP appointments were cancelled or how many ambulances and patients were diverted from the accident and emergency departments that were unable to treat patients.

1.9 NHS organisations did not report any cases of harm to patients or of data being compromised or stolen. If the WannaCry ransomware attack had led to any patient harm or loss of data then NHS England told us that it would expect trusts to report cases through existing reporting channels, such as reporting data loss direct to the Information Commissioner's Office (ICO) in line with existing policy and guidance on information governance. NHS Digital also told us that analysis of the WannaCry ransomware suggested that the cyber attack was not aimed at accessing or stealing data, although it does not know for certain that this is the case.

1.10 The NHS continued to provide emergency care from 12 May to 19 May, although some patients had to travel further as five hospitals had diverted services (paragraph 1.7). Patients with planned appointments experienced most disruption. Cancer charities, including Macmillan Cancer Support and Cancer Research UK, reported cancellations causing distress to patients. NHS England's own review identified at least 139 patients who had an urgent referral for potential cancer cancelled, as at 18 May, although the actual number may be higher if trusts misreported during the data collection or identified cancellations after 18 May.

The financial impact

1.11 The Department of Health (the Department), NHS England and the National Crime Agency have told us that no NHS organisations paid the ransom. NHS Digital told us it advised against the payment of the WannaCry ransom during site visits and telephone conferences with infected trusts. Furthermore, NHS England and NHS Digital wrote to all trusts on 14 May advising them against the payment of ransoms, but these emails did not always reach trusts after that attack had begun.

1.12 The NHS has not calculated the total cost of cancelled appointments; of NHS staff overtime; of additional IT support provided by NHS local bodies or IT consultants; or the cost of restoring data and systems affected by the attack. For example, trusts and other NHS organisations had to roll back systems and restore data and systems, including re-entering data recorded manually while trusts' systems were down. National and local NHS staff had to work overtime, including over the weekend of 13–14 May, to resolve problems and to prevent a fresh wave of organisations being affected by WannaCry on Monday 15 May.

The recovery

1.13 In line with its established procedures for responding to a major incident, NHS England focused its initial response on maintaining emergency care, and within 24 hours began attending to primary care. Since the attack occurred on a Friday it caused minimal disruption to primary care services, which tend to be closed over the weekend. Twenty-two of the 27 infected acute trusts continued treating urgent and emergency patients throughout the weekend. However, five trusts, including Barts Health NHS Trust, were unable to see some patients and had to divert them to other hospitals, and a further two needed outside help to continue treating patients. NHS England worked with trusts to ensure diverts were put in place and help provided. By Tuesday 16 May, only two hospitals were still diverting patients: Lister Hospital in Hertfordshire and Broomfield Hospital in Essex. NHS England 'stood down' the incident on Friday 19 May.

1.14 The recovery was aided by the work of a cyber-security researcher who activated a kill-switch so that WannaCry stopped locking devices. The researcher triggered the kill-switch on the evening of Friday 12 May. This meant that some NHS organisations were infected by the WannaCry malware, but because of the actions of the researcher they were not locked out of their devices and systems. Between 15 May and mid-September, NHS Digital and NHS England identified a further 92 organisations, including 21 trusts, attempting to contact the WannaCry domain, in addition to the initial 45 organisations they had identified as being infected. Although some of these trusts may have contacted the WannaCry domain as part of their cyber-security activity.

Part Two

Why some parts of the NHS were affected

2.1 NHS organisations across England were affected by the WannaCry attack. **Figure 3** sets out the location of the trusts affected and shows the:

- 37 trusts infected by the WannaCry malware; and
- 44 trusts not infected by the malware but reporting disruption.

2.2 Of the 37 trusts infected, 32 were located in the North NHS region and the Midlands and East NHS region. NHS England believes more organisations were infected in these regions because they were hit early on 12 May before the WannaCry kill-switch was activated.

Failure to patch and update systems and reliance on old software

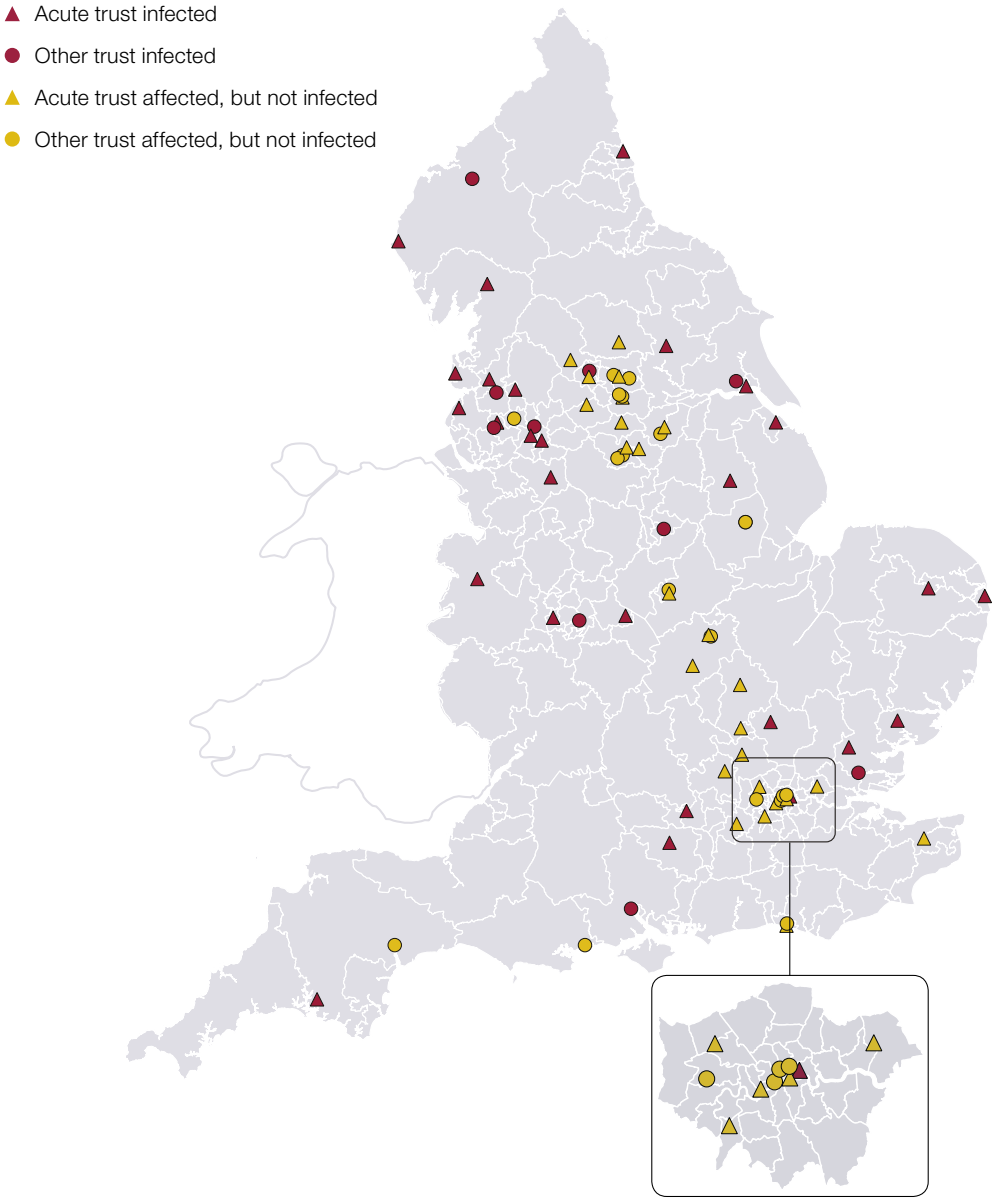
2.3 It is not possible to eliminate all cyber threats but organisations can prevent harm through good cyber-security. Such practice includes maintaining up-to-date firewalls and anti-virus software, and applying patches (updates) in a timely manner. NHS England's view is that WannaCry infected some parts of the NHS mainly because organisations had failed to maintain good cyber-security practices.

2.4 NHS Digital told us that all the infected trusts had a common vulnerability in their Windows operating systems which was exploited by the WannaCry attack. All NHS organisations infected by WannaCry had unpatched, or unsupported, Windows operating systems. However, whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded the organisations against infection.

Figure 3

Trusts affected by the cyber attack

Disruption to front-line services affected all parts of the country but was concentrated in the North NHS region and the Midlands and East NHS region



Note

1 NHS England believes the concentration of infected trusts in the North NHS region and the Midlands and East NHS region does not reflect variations in cyber-security, but may be partially explained by these organisations becoming infected earlier in the day, before the WannaCry 'kill-switch' was activated.

Source: National Audit Office analysis of NHS England data

2.5 NHS Digital told us that the majority of NHS devices infected were unpatched but on the supported Windows 7 operating system. Trusts using Windows 7 could have protected themselves against WannaCry by applying a patch (or update) issued by Microsoft in March 2017, and NHS Digital had issued CareCERT alerts on 17 March and 28 April asking trusts to apply the patch.[2] According to the Department of Health (the Department), more than 90% of devices in the NHS use the Windows 7 operating system.

2.6 A second issue was that some trusts were running the older Windows XP operating system on some devices. This made the trusts vulnerable because Microsoft was no longer releasing patches for this operating system, and so they could not protect their systems from WannaCry unless they isolated those devices from the network. Some trusts also experienced issues with some medical equipment, such as MRI scanners that have Windows XP embedded within them (see paragraph 1.3). This equipment is generally managed by the system vendors and local trusts are not capable of applying updates themselves. Support from the vendors of these devices was often poor according to NHS England and NHS Digital. However, trusts running Windows XP on their medical equipment could have protected themselves by isolating these devices from the rest of the network (although this may necessitate manual workarounds). In July 2017, as part of its response to the National Data Guardian review, the Department told local bodies to ensure that they had moved away from, or were actively managing, unsupported software by April 2018.

2.7 The Department and Cabinet Office had written to trusts in 2014 offering some temporary help with security for old equipment until April 2015, after which time there would be no support. This meant that it was essential that all NHS organisations had "robust plans" to migrate away from Windows XP. Despite this, the Department told us about 5% of the NHS IT estate, including computers and medical equipment, was still using Windows XP on 12 May 2017. This is partly explained by the fact that it is not always possible to remove or update Windows XP in applications and IT services based on that operating system. Immediately after the WannaCry attack Microsoft issued a patch for Windows XP that would prevent WannaCry and similar ransomware.

Leadership and size of trusts

2.8 We found no clear relationship between those trusts infected by WannaCry and the quality of their leadership, as rated by the Care Quality Commission (CQC). Of the 37 trusts infected by WannaCry, four (11%) had been rated as 'inadequate' against the 'well-led' domain at their last CQC inspection, compared with 7% of NHS organisations not infected.[3] However, CQC had not focused on how well led trusts were in relation to cyber-security in their inspections before 12 May 2017. We understand CQC has plans to enhance its line of questions regarding information and digital systems as part of its inspection of the leadership of trusts in the future.

2 A CareCERT alert is an email sent by NHS Digital providing information or requiring action from NHS organisations.
3 Of the 37 trusts infected by WannaCry, 36 had a CQC rating.

2.9 We also found that infected trusts tended to employ more staff than average. Of the 37 infected trusts:

- 14 (38%) were among the 25% of trusts employing the most staff; and
- 26 (70%) employed more than the median number of staff.

Although there is limited evidence on why this should be the case, we found that:

- some of the trusts we spoke to told us that integrating IT systems when trusts merge (and become larger) and running many different versions of Windows operating systems, not all of which are supported, can be a challenge; and
- WannaCry exploited weaknesses within parts of Microsoft's Windows operating system used to share files within organisations. This meant it spread automatically in some cases, and organisations with large Windows networks were among the worst affected.

Prepared for a cyber attack

2.10 Before 12 May, the Department and its arm's-length bodies did not know whether trusts had complied with CareCERT alerts as no formal mechanism of assessment existed at that time. On 12 May, NHS Digital worked with NHS England to put in place a formal mechanism for assessing whether NHS organisations had complied with CareCERT alerts. Emergency, Preparedness, Resilience and Response (EPRR) teams requested a positive return from providers by midnight on 12 May that, for example where they had:

- not been subject to an attack, they had implemented the patch; and
- been subject to an attack, they had implemented remedial works; had been able to roll back their systems; and could continue to provide emergency services or – if not – had put mitigations in place.

2.11 Before the WannaCry attack, NHS Digital offered an on-site inspection to hospitals to assess their cyber-security (known as 'CareCERT Assure'). This inspection was voluntary. By 12 May, NHS Digital had inspected 88 out of 236 trusts and none had passed. NHS Digital's review of the WannaCry attack concluded that CareCERT advice and guidance (including inspections) was mostly followed by organisations with relatively mature cyber-security arrangements, while vulnerable trusts were not taking action to improve their security. NHS Digital also found that, in general, trusts had not identified cyber-security as being a risk to patient outcomes, and had tended to overestimate their readiness to manage a cyber attack. NHS Digital believes this reflects a lack of understanding of the nature of cyber risk among trusts, rather than a neglect of cyber-security.

2.12 The Department and its arm's-length bodies did not hold information on how prepared local organisations were to respond to a cyber attack, such as whether cyber-security appeared on organisations' risk registers or whether trusts complied with good practice. The Department and its arm's-length bodies also had limited central information on trusts' IT and digital assets such as anti-virus software and IP addresses. At the start of its investigation, the National Crime Agency had to gather evidence from all sites, including information on the devices affected, IP addresses and network traffic, to assess the impact of WannaCry on the NHS, rather than being able to access the information centrally.

Part Three

How the Department and the NHS responded

Devolved responsibility for cyber-security

3.1 The Department of Health (the Department) has overall national responsibility for cyber-security resilience and responding to incidents in the health sector. However, the Department devolves responsibility for managing cyber-security to local organisations – NHS trusts, GPs, clinical commissioning groups and social care providers. Regulators and other national bodies oversee and support local NHS organisations. While NHS foundation trusts are directly accountable to Parliament for delivering healthcare services, they are held to account by the same regulators as NHS trusts. Roles and responsibilities for cyber-security as at September 2017 are set out in **Figure 4** on pages 22 and 23. In particular:

- NHS Improvement holds trusts and NHS foundation trusts to account for delivering value for money; and
- the Care Quality Commission (CQC) regulates health and social care providers for safety and quality of their services.

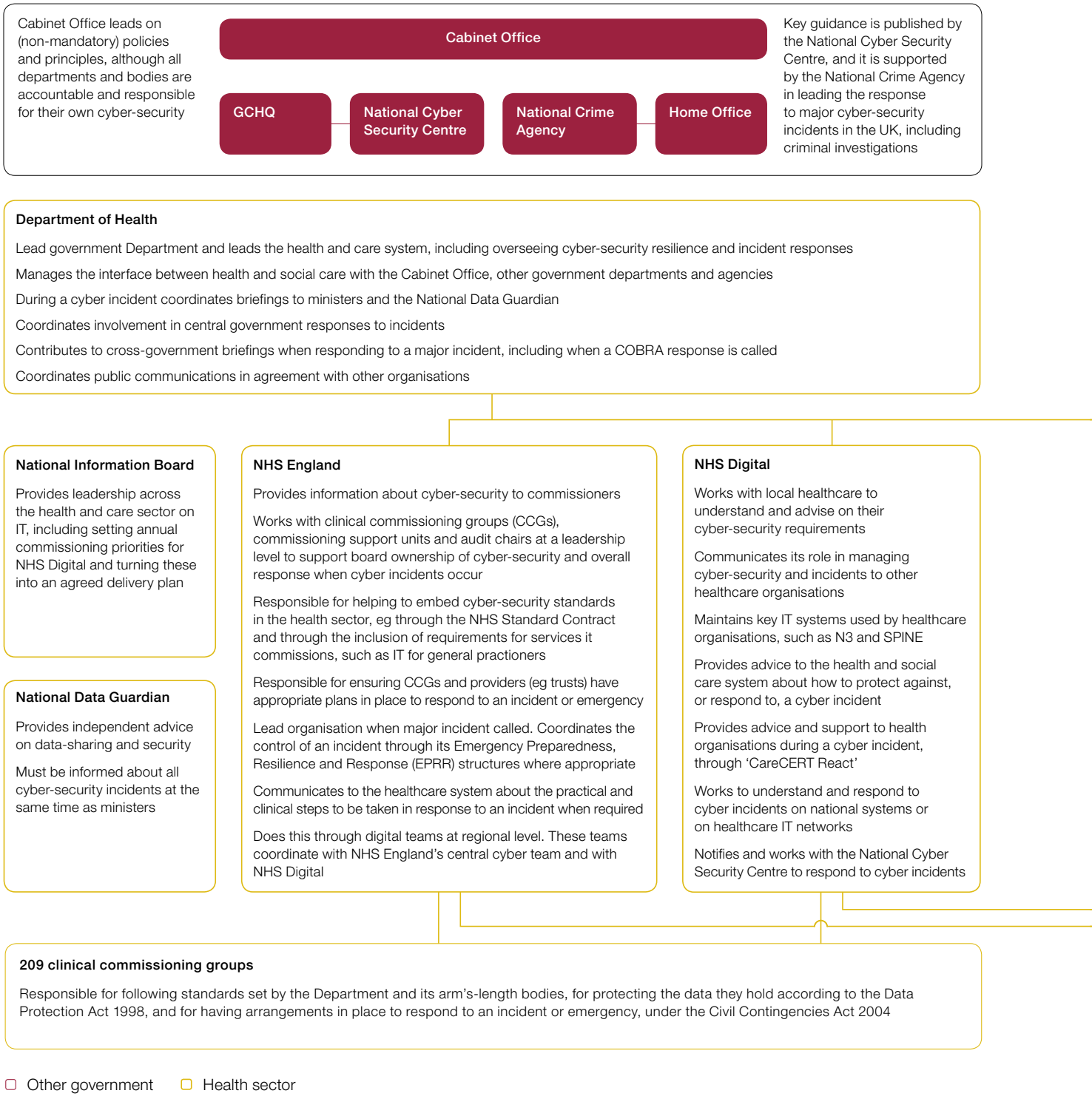
3.2 Both bodies can mandate local NHS organisations to improve their performance. They also have a role in ensuring that local bodies have appropriate cyber-security arrangements, but neither are primarily concerned with cyber or information technology issues. NHS Digital provides guidance, alerts and support to local organisations on cyber-security, and can visit organisations to evaluate cyber-security arrangements if asked to do so, as part of CareCERT Assure.[4] However, NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of that organisation.

4 Prior to the WannaCry attack, NHS Digital offered an on-site inspection to hospitals to assess their cyber-security. This was known as 'CareCERT Assure' and was voluntary. NHS national bodies are currently revising this system.

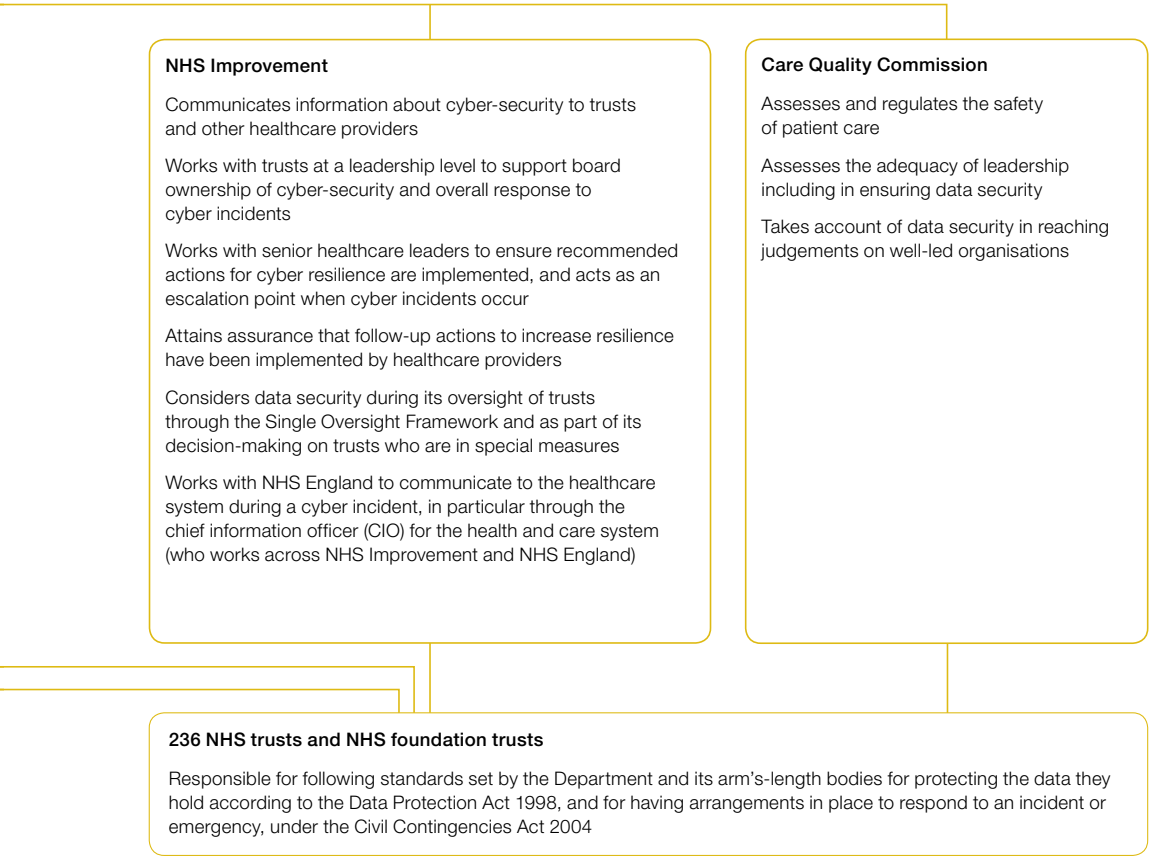
Figure 4

Roles and responsibilities for cyber-security in the NHS as at September 2017

National and local bodies share responsibility for cyber-security in the health sector



Source: National Audit Office analysis of Department of Health and NHS England data


NHS Improvement
Communicates information about cyber-security to trusts and other healthcare providers
Works with trusts at a leadership level to support board ownership of cyber-security and overall response to cyber incidents
Works with senior healthcare leaders to ensure recommended actions for cyber resilience are implemented, and acts as an escalation point when cyber incidents occur
Attains assurance that follow-up actions to increase resilience have been implemented by healthcare providers
Considers data security during its oversight of trusts through the Single Oversight Framework and as part of its decision-making on trusts who are in special measures
Works with NHS England to communicate to the healthcare system during a cyber incident, in particular through the chief information officer (CIO) for the health and care system (who works across NHS Improvement and NHS England)
Care Quality Commission
Assesses and regulates the safety of patient care
Assesses the adequacy of leadership including in ensuring data security
Takes account of data security in reaching judgements on well-led organisations
236 NHS trusts and NHS foundation trusts
Responsible for following standards set by the Department and its arm's-length bodies for protecting the data they hold according to the Data Protection Act 1998, and for having arrangements in place to respond to an incident or emergency, under the Civil Contingencies Act 2004

How the cyber attack was managed

3.3 Before the WannaCry attack the Department had developed a plan for responding to a cyber attack, which included roles and responsibilities of national and local organisations. However, the Department had not tested the plan at a local level. This meant the NHS was not clear what actions it should take when affected by WannaCry, including how it should respond at a local level. On 12 May 2017, NHS England determined that it should declare a national major incident and decided that it would lead the response, coordinating with NHS Digital and NHS Improvement. NHS England treated the attack as a major operational incident through its existing Emergency Preparedness, Resilience and Response (EPRR) processes. However, as NHS England had not rehearsed its response to a cyber attack it faced a number of challenges. The cyber attack was less visible than other types of incident and not confined to local areas or regions in the way a major transport accident would have been, for example. This meant that it took more time to determine the cause of the problem, the scale of the problem and the number of people and organisations affected.

3.4 Without clear guidelines on responding to a national cyber attack, organisations reported the attack to different sources including the local police, NHS England and NHS Digital. For the same reason communications to patients and local organisations also came from a number of sources. These included the National Cyber Security Centre, which was providing support to all UK organisations affected by the attack, NHS England and NHS Digital. In addition, the use of email for communication was limited, although NHS Improvement did communicate with trusts' chief executive officers by telephone. Affected trusts shut down IT systems, including some trusts disconnecting from NHS email and the N3 network as a precautionary measure.[5] The Department coordinated the response with the centre of government, briefing ministers, liaising with the National Cyber Security Centre and National Crime Agency, and overseeing NHS England's and NHS Digital's operational response.

3.5 Affected trusts were triaged through the EPRR route and, where necessary, received assistance from national bodies, including advice and physical technical support from NHS Digital, which sent 54 staff out to hospitals to provide direct support. Staff at the Department, NHS England, NHS Improvement and NHS Digital, as well as large numbers of staff in other organisations across the NHS, worked through the weekend to resolve the problem and avoid further problems on Monday. NHS England's IT team did not have on-call arrangements in place, but staff came in voluntarily to help resolve the issue. Front-line NHS staff adapted to communication challenges and shared information through personal mobile devices, including using the encrypted WhatsApp application. NHS national bodies and trusts told us that this worked well on the day although is not an official communication channel.

5 N3 is the broadband network connecting all NHS sites in England.

The risk of a cyber attack had been identified before WannaCry

3.6 The Secretary of State for Health asked the National Data Guardian and CQC to undertake reviews of data security. These reports were published in July 2016 and warned the Department about the cyber threat and the need for the Department to respond to it. They noted the threat of cyber attacks not only put patient information at risk of loss or compromise but also jeopardised access to critical patient record systems by clinicians. They recommended that all health and care organisations needed to provide evidence that they were taking action to improve cyber-security, such as through the 'Cyber Essentials' scheme.[6]

3.7 Although WannaCry was the largest cyber-security incident to affect the NHS, individual NHS organisations had been victims of other attacks in recent years (**Figure 5** overleaf). WannaCry infected one of England's biggest trusts, Barts Health NHS Trust. This was the second cyber attack to affect the trust in six months. A ransomware attack had also affected Northern Lincolnshire and Goole NHS Foundation Trust in October 2016, which had led to it cancelling 2,800 appointments.

Lessons learned

3.8 The NHS has accepted that there are lessons to learn from WannaCry and is already taking action. The NHS has identified the need to improve the protection of services from future cyber attacks. These include the need to:

- develop a response plan setting out what the NHS should do in the event of a cyber attack and establish the roles and responsibilities of local and national NHS bodies and the Department;
- ensure organisations implement critical CareCERT alerts, including applying software patches and keeping anti-virus software up to date and identifying;
- ensure essential communications are getting through during an incident when systems are down; and
- ensure that organisations, boards and their staff are taking the cyber threat seriously, understand the direct risks to front-line services and are working proactively to maximise their resilience and minimise the impact on patient care.

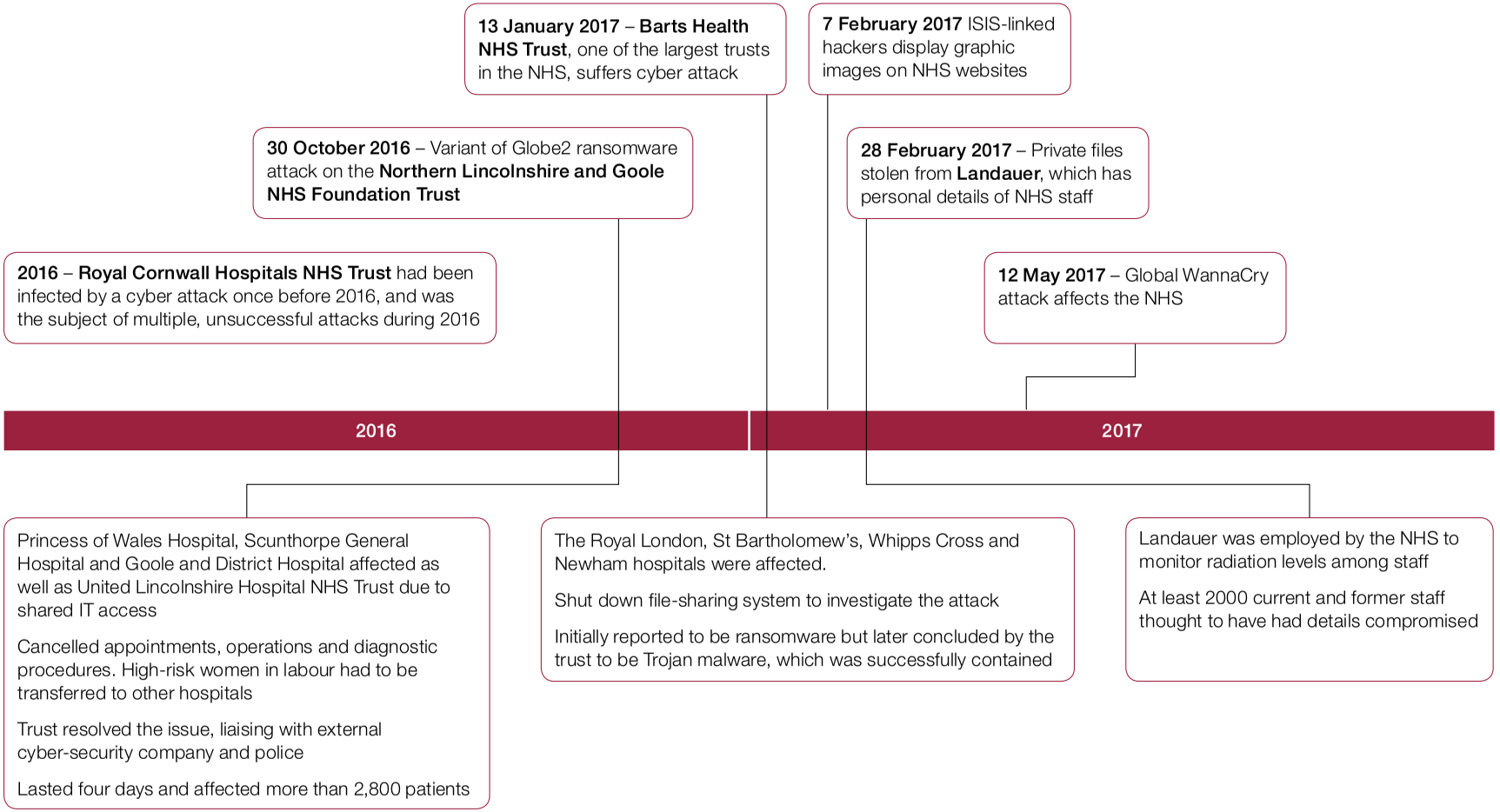
3.9 Following the WannaCry attack, NHS England and NHS Improvement wrote to every trust, clinical commissioning group and commissioning support unit asking boards to ensure that they had implemented all 39 CareCERT alerts issued by NHS Digital between March and May 2017 and had taken essential action to secure local firewalls.

6 Cyber Essentials is a government-designed cyber-security certification scheme that sets out a baseline of cyber-security and can be used by any organisation in any sector, see: www.cyberaware.gov.uk/cyberessentials/

Figure 5

Cyber attacks on the NHS in 2016 and 2017 before 12 May 2017

The NHS had experienced a number of cyber attacks prior to the WannaCry attack



Source: National Audit Office

3.10 NHS England and NHS Improvement are talking to every major trauma centre and ambulance trust, and will reprioritise £21 million in capital funding from existing IT budgets to improve cyber-security in major trauma centres. NHS Digital has built a new CareCERT Collect portal to provide assurance that trusts have implemented cyber alerts and to collect central data on IT and digital assets in the NHS. Since 2015, the Department has made £50 million available to provide central support to the health and care system through the CareCERT suite of services.

3.11 Following the WannaCry attack, in July 2017 the Department published its response to the National Data Guardian and CQC recommendations. The response built on existing work to strengthen cyber-security in the NHS, involving the Department and its arm's-length bodies. For example, NHS Digital was developing its existing services to support local organisations, including broadcasting alerts about cyber threats, providing a hotline for dealing with incidents, sharing best practice across the health system and carrying out on-site assessments to help protect against future cyber attacks; and NHS England had embedded the 10 Data Security Standards, recommended by the National Data Guardian, in the standard NHS contract for 2017-18, and was providing training to its Board and local teams to raise awareness of cyber threats. The Department also told us that a revised version of the Information Governance Toolkit is being developed for use in 2018-19, and that the inspection framework used by the CQC will be updated to incorporate the data standards.[7]

7 The Information Governance Toolkit draws together the legal rules and central guidance issued by the Department of Health, and presents them in a single standard as a set of information governance requirements. All health and social care providers, commissioners and suppliers are required to carry out self-assessments of their compliance against these requirements. The Toolkit is commissioned by the Department and is maintained by NHS Digital. See www.igt.hscic.gov.uk/

Appendix One

Our investigative approach

Scope

1 We conducted an investigation into the WannaCry cyber attack that affected the NHS in England on 12 May 2017. We investigated:

- the WannaCry attack's impact on the NHS and its patients;
- why some parts of the NHS were affected; and
- how the Department, NHS national bodies (NHS England, NHS Digital and NHS Improvement) and other national bodies, such as the National Cyber Security Centre and National Crime Agency, responded to the incident.

Methods

2 In examining the issues in paragraph one, we drew on a variety of evidence sources.

3 We conducted semi-structured interviews with officials from:

- Department of Health
- NHS England
- NHS Digital
- NHS Improvement
- Care Quality Commission
- National Cyber Security Centre
- National Crime Agency
- Cabinet Office.

4 We visited four local trusts to examine their roles and responsibilities in relation to cyber-security; the impact of WannaCry on the trust and its patients; and how the trust responded to the incident:

- Barts Health NHS Trust;
- Bedford Hospital NHS Trust;
- Northern Lincolnshire and Goole NHS Foundation Trust; and
- the Royal Marsden NHS Foundation Trust.

5 We reviewed documents relating to the WannaCry ransomware attack including documents setting out roles and responsibilities for cyber-security in the NHS and across the wider public sector. We also reviewed published and unpublished research and reports relating to the NHS and WannaCry and cyber-security more generally.

6 We carried out analysis of data provided by NHS England, NHS Digital and the Care Quality Commission.

Appendix Two

Trusts infected or disrupted by WannaCry

Figure 6

Trusts infected, or affected, by the WannaCry attack

Trusts infected by WannaCry, and locked out of devices

Barts Health NHS Trust

Birmingham Community Healthcare NHS Foundation Trust

Blackpool Teaching Hospitals NHS Foundation Trust

Bradford District Care NHS Foundation Trust

Bridgewater Community Healthcare NHS Foundation Trust

Central Manchester University Hospitals NHS Foundation Trust

Colchester Hospital University NHS Foundation Trust

Cumbria Partnership NHS Foundation Trust

East and North Hertfordshire NHS Trust

East Cheshire NHS Trust

East Lancashire Teaching Hospitals NHS Trust

Essex Partnership University NHS Foundation Trust

George Eliot Hospital NHS Trust

Greater Manchester Mental Health NHS Foundation Trust

Hampshire Hospitals NHS Foundation Trust

Hull and East Yorkshire Hospitals NHS Trust

Humber NHS Foundation Trust

James Paget University Hospitals NHS Foundation Trust

Lancashire Care NHS Foundation Trust

Lancashire Teaching Hospital NHS Trust

Mid Essex Hospital Services NHS Trust

Norfolk and Norwich University Hospital NHS Foundation Trust

North Cumbria University Hospitals NHS Trust

Northern Lincolnshire and Goole NHS Foundation Trust

Northumbria Healthcare NHS Foundation Trust

Nottinghamshire Healthcare NHS Foundation Trust

Plymouth Hospitals NHS Trust

Royal Berkshire Hospital NHS Foundation Trust

Salford Royal NHS Foundation Trust

Shrewsbury and Telford Hospital NHS Trust

Solent NHS Trust

Southport and Ormskirk Hospital NHS Trust

The Dudley Group NHS Foundation Trust

United Lincolnshire Hospitals NHS Trust

University Hospitals of Morecambe Bay NHS Foundation Trust

Wrightington, Wigan and Leigh NHS Foundation Trust

York Teaching Hospitals NHS Foundation Trust

Source: NHS England

Trusts not infected by WannaCry but known to have experienced disruption

Airedale NHS Foundation Trust

Ashford and St Peters Hospitals NHS Foundation Trust

Barking, Havering and Redbridge University Hospitals NHS Trust

Barnsley Hospital NHS Foundation Trust

Bedford Hospital NHS Trust

Bradford Teaching Hospitals NHS Foundation Trust

Brighton and Sussex University Hospitals NHS Trust

Buckinghamshire Healthcare NHS Foundation Trust

Calderdale and Huddersfield NHS Foundation Trust

Central London Community Healthcare NHS Trust

Chelsea and Westminster Hospital NHS Foundation Trust

Doncaster and Bassetlaw Hospitals NHS Foundation Trust

Dorset Healthcare NHS Foundation Trust

East Kent Hospitals University NHS Foundation Trust

Great Ormond Street Hospital NHS Foundation Trust

Guy's and St Thomas' NHS Foundation Trust

Harrogate and District NHS Foundation Trust

Kettering General Hospital NHS Foundation Trust

Kingston Hospital NHS Trust

Leeds and York Partnership NHS Foundation Trust

Leeds Community Healthcare NHS Trust

Leeds Teaching Hospitals NHS Trust

Leicestershire Partnership NHS Trust

Lincolnshire Community Health Services NHS Trust

Lincolnshire Partnership NHS Trust

London North West Healthcare NHS Trust

Luton and Dunstable NHS Trust

Mid Yorkshire Hospitals NHS Trust

Moorfields Eye Hospital NHS Foundation Trust

North West Ambulance Service NHS Trust

Northampton General Hospital NHS Trust

Northamptonshire Healthcare NHS Foundation Trust

Rotherham, Doncaster and South Humber NHS Foundation Trust

Sheffield Children's NHS Foundation Trust

Sheffield Health and Social Care NHS Foundation Trust

Sheffield Teaching Hospitals NHS Foundation Trust

South West Yorkshire Partnership NHS Foundation Trust

South Western Ambulance Service NHS Foundation Trust

Sussex Community NHS Foundation Trust

The Rotherham NHS Foundation Trust

University Hospitals of Leicester NHS Trust

West Hertfordshire Hospitals NHS Trust

West London Mental Health NHS Trust

Yorkshire Ambulance Service NHS Trust

Source: NHS England

This report has been printed on Evolution Digital Satin and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Design and Production by NAO External Relations
DP Ref: 11594-001

£10.00

ISBN 978-1-78604-147-0

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu