

AUGUST 2018

PARLIAMENT STREET

partnership in policy

NHS DATA SECURITY

PROTECTING PATIENT RECORDS





INTRODUCTION

An institution under attack

The National Health Service (NHS) is one of the most important services that we offer as a nation. Throughout the last 70 years of the NHS, the British public have continuously relied on the access to free healthcare and understood the importance of it remaining free and accessible for all.

The nurses and doctors in the NHS do a fantastic job curing the sick, despite challenging environments and huge budget constraints they face every day.

Due to the importance of the NHS, it is unfortunately often the target for negative publicity and, more importantly malicious cyberattacks.

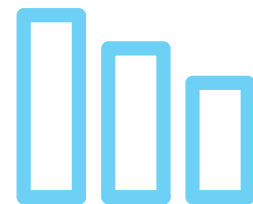
Hospitals are often a target because of the personal data they hold and the risk to lives lost, thanks to incorrect information or wrong medication. With the nature of the data that they hold, it could easily be seen as a goldmine for hackers wanting to steal precious patient data and upset the structure.

One of the largest, and arguably most famous cyberattacks on the NHS was the WannaCry attack in 2017.

Coined as the 'biggest ransomware' offensive in history, the global attack infected more than 300,000 computers in 150 countries and meant that 6,900 appointments had to be cancelled.

Whilst the scale of this issue was huge, it later came out that the attack on the NHS could have been prevented if the correct security recommendations had been followed. After the WannaCry attack, the NHS pledged £150m to bolster its defences against the growing threat of cyberattacks.

Another issue the NHS has faced more recently is the loss of 162,000 missing documents, along with the 702,000 pieces of paperwork already known to have been lost. This particular issue that the NHS faces questions the integrity of the software they have in place and the security of paper documents.



METHODOLOGY

An overview of our research approach

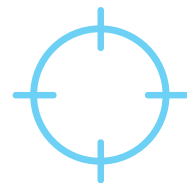
The Parliament Street research team liaised with 68 NHS Trusts for this study.

The team asked for information on patient records which were reported 'missing' over the last financial year. In addition our researchers asked for detail on whether hand-written records were used within each hospital and which IT systems were being used to manage patient records.

It is important to note that some NHS Trusts provided data on records which were originally thought to be missing, but were retrieved at a later date. All extra notes have been included in this report for the purposes of clarity of the situation.

All information was sourced under Freedom of Information (FOI) legislation and returned in June 2018.





SECURITY FEARS

The recent examples of the struggles the NHS has gone through has influenced public attitude towards the health service. Data and security is a vital element for the NHS, not just to protect the data they hold, but to continue to have public trust in the system and keep their confidential data secure.

The public are of course sceptical of any service that holds their private, personal data but are finding it increasingly difficult to trust the NHS.

After it was revealed that a large number of NHS organisations were running out-of-date Windows XP software – an unsophisticated software for blocking malicious malware, trust in the capabilities of the NHS and the government's ability to fund the service dipped significantly.

However, recent research from Heathwatch has found that while the issues the NHS has faced over the past year have been significant, more than three quarters of the British public say they trust the NHS with handling their private data.

The research also found that 73 per cent of the public would be happy for the NHS to use their personal information to improve on the healthcare service they provide. These statistics into public trust are interesting as they clearly show the public are still behind the NHS, despite the issues faced.

This could potentially be due to the public shifting the blame onto the government for the cuts the NHS have faced, rather than the responsibility being placed directly onto the NHS.

Interestingly, this research did find more than half of the people surveyed had concerns around how their information was used in the NHS, thus meaning there is real concern with the public as to where their data is going and who will have access to it. This could be encouraged by the significant use of paper notes and handwritten prescriptions in the health service. It is clear from the recent data loss that paper notes are not a secure way of storing crucial patient information.





DATA ANALYSIS

Biggest incidents of 'unavailable' patient records in the most recent financial year

3,179 UNIVERSITY HOSPITAL BIRMINGHAM

2,163 BOLTON NHS TRUST

1,105 UNIVERSITY HOSPITAL BRISTOL

Total reported losses from the 68 hospitals that responded to the request for information

9,132
MISSING PATIENT
RECORDS

94%
USE HANDWRITTEN
NOTES

The Parliament Street research team liaised with 68 NHS hospital trusts through the Freedom of Information Act (FOI) to request data into lost or stolen patient records.

Many of the trusts included in their responses the amount of records that were unable to be found upon patient request in the given time frame.

It is important to note that the 9,132 documents that were reported unavailable or lost also includes many incidents where the files were eventually located.

When asked whether the trust still uses handwritten notes, the research team discovered 94 per cent of trusts still use this method of documentation. The FOI request was dated for financial year 2017-18.

Our research team discovered that in the last financial year, the University Hospital Birmingham reported the largest amount of records 'unavailable' for out patient clinic appointments at a staggering 3,179 documents, despite using electronic clinical systems such as iCARE and Concerto.

The second largest figure was Bolton NHS Trust who were unable to provide 2,163 records in time of the patient appointment and use LE 2.2 Patient Management System to record their data.

PATIENT SECURITY



The third largest trust with missing patient data is University Hospital Bristol which reported 1,105 incidents of records being unavailable however it is worth noting that 1,075 of these were found at a later date.

Wigan and Leigh NHS Foundation Trust were the fourth highest with 426 records of patient data being lost. Interestingly, the fifth highest was the Royal Devon and Exeter NHS Foundation Trust who reported they had 425 cases of lost or stolen data and do not use an electronic system to hold the information, with records being held in paper case notes.

It is also worth noting that out of the 68 NHS hospital trusts, only 16 of those reported that there were no cases of lost or stolen patient data, with many reporting they still had missing records.

As well as this, West Suffolk NHS Foundation Trust specifically reported that they had a record of a patient list which had been stolen, despite using Cerner Millennium as an electronic source to hold data.

RECOMMENDATIONS

1. Abolish handwritten notes in hospitals

The process of developing patient records through handwritten notes may be convenient, but it inevitably leads to errors and potential security issues. For example, individual handwriting styles can be misinterpreted, leading to incorrect information being collated and acted upon. The use of paper files also exposes documents to the risk of loss or damage, something highly likely to occur in a busy hospital environment.

It is clear that paper-based systems are no longer fit for purpose and NHS Trusts should work towards implementing digital systems with records capture via tablet computers and mobile devices.

2. Introduce a patient identity protocol

With nearly 10,000 patient records reported as missing in the last year, it's clear that much more needs to be done to protect the identity and integrity of patient documents. Patients should, for example, have up to date information about the status of their records, and the ability to access notes and updates from health professionals online. One way of doing this could be to introduce speech recognition software so that GPs, midwives and other professionals could quickly capture digital notes from consultations.

It is important that patient processes are improved, so a patient identity protocol could help raise standards across NHS Trusts, ensuring all information is properly captured and stored digitally. This would greatly increase the security and privacy protection for patients.