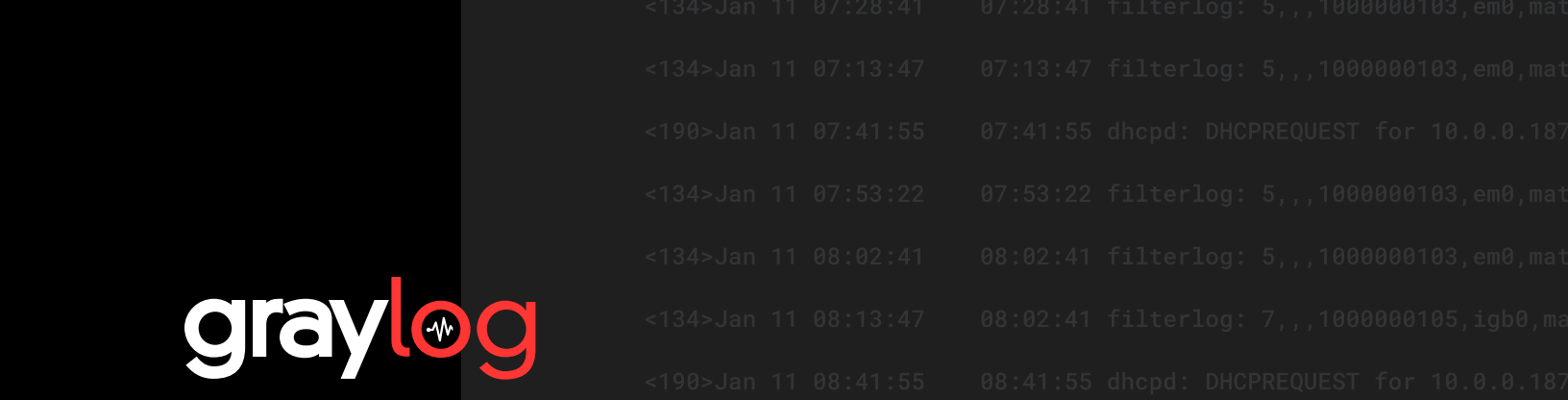


graylog

GRAYLOG FOR NATIONAL HEALTH SERVICES

TABLE OF CONTENTS

INTRODUCTION

Managing patient care in a digitally transformed era is increasingly difficult. National Health Services (NHS) trusts seek to provide the best patient care possible, but the need to share electronic healthcare data securely remains a challenge.

NHS trusts need to share data across disparate electronic systems, but the ability of these systems to communicate with one another while maintaining data security and privacy remains a struggle. In their January 2020 article, "Interoperability in NHS hospitals must be improved: the Care Quality Commission should be a key actor in this process," the authors note that while interoperability is vitally important to reduce the administrative data gathering burden for clinicians and enable well-curated research datasets.[1] Also, a recent independent survey on NHS interoperability indicated that 33% of respondent trusts could not electronically access outside patient data.[2]

Despite the public health benefits associated with interoperability, governance surrounding data-sharing requires the trusts to consider the management and use of linked data, particularly in preventing unauthorised access. Looking for a single source of guidance in managing patient data becomes increasingly difficult as data types increase along with governing bodies. For example, according to a 2020 research paper by the Royal Society, various trusts have distributed data governance research around data ethics, data privacy and anonymisation, data-sharing and interoperability, data protection and security, and responsible innovation, including [3]:

- Nuffield Council on Bioethics
- British Standards Institute
- Ada Lovelace Institute and Understanding Patient Data

[1] Zhang, J., Sood, H., Harrison, O. T., Horner, B., Sharma, N., & Budhdeo, S. (2020). "Interoperability in NHS hospitals must be improved: the Care Quality Commission should be a key actor in this process." *Journal of the Royal Society of Medicine*, 113(3), 101–104. https://doi.org/10.1177/0141076819894664

[2] Ibid.

[3] The Royal Society. (2020, June). *The UK data governance landscape: Explainer.* https://royalsociety.org/-/media/policy/projects/data-governance/uk-data-governance-explainer.pdf?la=en-GB&hash=1FFB10307A248739C9207D23743E152D

- Department of Health and Social Care
- Reform
- National Health Services
- Centre for Data Ethics and Innovation
- National Data Guardian for Healthcare

Embracing digital transformation and creating interoperability across the NHS system is mission-critical. With that in mind, trusts need to find IT solutions that enable digital and physical health.

NHS TRUSTS CALL 999: DATA SHARING AND SECURITY

Healthcare is an industry that relies on stakeholder trust. Unlike commerce or banking, patients expect their healthcare providers to have their best interests at heart. New doctors swear an oath as members of the medical profession, one that includes "I will respect the autonomy and dignity of my patients, and will uphold their confidentiality."[4]

> "I will respect the autonomy and dignity of my patients, and will uphold their confidentiality."
>
> Hippocratic Oath

In today's digital world, upholding confidentiality involves ensuring electronic data security and privacy.

[4] *Hippocratic Oath | Graduation | University of Exeter*. (2021). University of Exeter. https://www.exeter.ac.uk/graduation/bmbs/hippocraticoath/

DATA SHARING IN NHS

Not only must trusts share data as part of healthcare management, but sharing electronic healthcare data with private technology companies, including genomics medicine and artificial intelligence (AI) companies. In the article, "Sharing whilst caring: solidarity and public trust in a data-driven healthcare system," [5] the authors note that data sharing with the private sector must sit on a foundation of trust to maintain the relationship between patient and provider.

The article specifically notes,

> **The introduction of laws and regulations can go some way to convince people that their interests are protected.... The pursuit of collective interests and the common good seems crucial to the establishment and preservation of trust that needs to sit alongside strict regulations as offered by e.g. the EU General Data Protection Regulation or the Big Data Task Force of European Medicines Agencies and the Heads of Medicines Agencies.[6]**

Ultimately, the more NHS trusts share data with external, private technology companies, the more laws will seek to codify security and privacy. These laws intend to solidify trust between patients and their healthcare providers, yet they create a burden on trusts whose budgets often fail to provide them with the resources necessary for ensuring compliance.

Inequality is a common theme across all data around NHS trust cybersecurity and technology. Trusts deploy interoperability inequitably, and the same is true for IT and cybersecurity staffing across trusts. Although the NHS has managed to reduce the cybersecurity skills gap,

---

[5] Horn, R. (2020, November 3). *Sharing whilst caring: solidarity and public trust in a data-driven healthcare system.* BMC Medical Ethics. https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-020-00553-8

[6] *Ibid.*

it has created divergent outcomes. According to a 2021 article in *Infosecurity Magazine*, one expert noted:[7]

> **"It's easy to assume that trusts of a similar size would have similar security strategies and budgets. However, it's clear that they operate in very different ways when it comes to security. Some trusts employ many qualified professionals. Others have none and, in some cases, may choose to outsource all of their security functions."**

This disparity in staffing equates to a disparity in cybersecurity, placing patient data at risk and trusts at a significant disadvantage compared to cybercriminals.

DATA SECURITY BY THE NUMBERS

Given the wealth of information that a single electronic health record contains, no one should be surprised that it remains a continued target for cybercriminals. A quick look at the data security statistics proves that malicious actors continue to push for patient data, even during a global health crisis.

The numbers provided by the National Cyber Security Centre (NCSC) bear out the continued data security concerns in healthcare during 2020[8],

- **160+:** high-risk and critical vulnerabilities shared with NHS trusts
- **200:** related to coronavirus investigated by NCSC
- **230:** victims facing incidents related to coronavirus

---

[7] Muncaster, P. (2021, March 31). *NHS Reduces Cyber-Skills Shortages but Breach Problems Remain.* Infosecurity Magazine. https://www.infosecurity-magazine.com/news/nhs-cyber-skills-shortages-breach/

[8] *NCSC – 2020 Annual Review.* (2020). NCSC. https://www.ncsc.gov.uk/annual-review/2020/index.html

- **235:** Active Cyber Defense (ACD) services released, including Web Check, Mail Check, and protective DNS
- **51,000:** Indicators of Compromise (IoCs) shared with NHS
- **1 million+:** IP addresses scanned while looking for security weaknesses
- **1.4 million:** NHS endpoints that had threat hunting performed on them to detect suspicious activity

Malicious actors continued to target overburdened trusts even as they struggled to manage increasing numbers of COVID-19 cases, finding themselves overwhelmed and understaffed.

DOING MORE WITH LESS

Despite the push for interoperability and the increasing demand to share patient data to enhance medical research, NHS lacks the ability to provide adequate funding to support these initiatives.

According to a May 15, 2020, report by the National Audit Office titled "Digital transformation in the NHS," the government expenditure through the Digital Transformation Portfolio included £4.7 billion between 2016-17 and 2020-21. However, cost estimates indicated that NHS would need around £8.1 billion to deliver digital transformation ambitions. [9]

Problematically, the same report notes that since the WannaCry attack in 2017, on-site assessments using the Cyber Essential Plus standards indicates that as of February 2020, 204 of the 236 trusts had been assessed with an average score of 63% – only a slight improvement over the estimated average score of 50% from late-2017.[10] Moreover, despite Cyber Essentials Plus requiring 100% for a trust to pass the assessment, only one trust achieved that. [11] Although compliance is not equal to security, these numbers indicate cybersecurity health and hygiene problems that will ultimately spread to their patients.

---

[9] Comptroller and Auditor General. (2020, May 15). *Digital transformation in the NHS.* National Audit Office. https://www.nao.org.uk/wp-content/uploads/2019/05/Digital-transformation-in-the-NHS.pdf

[10] *Ibid.*

[11] *Ibid.*

COMPLIANCE IS A BANDAID, NOT A VACCINE

With greater focus on NHS trust cybersecurity, the UK government places increasing stress on the need for stronger controls protecting patient data. In an attempt to provide guidance, the NHS released the Data Security and Protection Toolkit in 2020, and the NCSC released new versions of the Cyber Essentials scheme certification.

Although the two appear divergent, they have significant overlaps. Thus, trusts seeking to mature their cybersecurity posture should look to both of these compliance schemes as a way to enhance their controls and protect patient data.

The "Cyber Essentials: Requirements for IT infrastructure" [12] specifies five technical control themes. Meanwhile, Digital Data Security and Protection Toolkit [13] (DSP Toolkit) takes a more in-depth approach, establishing ten security standards with various assertions within each.

[12] National Cyber Security Centre. (2021). *Cyber Essential Requirements for IT Infrastructure 2.2.* Cyber Essentials: Requirements for IT Infrastructure. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-2.pdf

[13] National Health Service. (2020, September). *Strengthening Assurance: Data Security and Protection (DSP) Toolkit Independent Assessment Framework.* https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides

A comparison between the two cybersecurity frameworks gives greater visibility into their similarities:

Cyber Essentials Scheme	Data Security and Protection Toolkit
Firewalls Ensure that only safe and necessary network services can be accessed from the Internet.	**Data Security Standard 9 Assertion 7** The organisation is protected by a well-managed firewall.
Secure configuration Ensure that computers and network devices are properly configured to: • reduce the level of inherent vulnerabilities • provide only the services required to fulfil their role	**Data Security Standard 9 Assertion 6** You securely configure the network and information systems that support the delivery of essential services.
User access control Ensure user accounts: • are assigned to authorised individuals only • provide access to only those applications, computers, and networks required for the user to perform their role	**Data Security Standard 4 Assertions 1-5** The organisation maintains a current record of staff and their roles. Organisation assures good management and maintenance of identity and access control for its networks and information systems. All staff understands that their activities on IT systems will be monitored and recorded for security purposes. You closely manage privileged user access to networks and information systems supporting the essential service. You ensure your passwords are suitable for the information you are protecting.
Malware protection Restrict execution of known malware and untrusted software to prevent harmful code from causing damage or accessing sensitive data.	**Data Security Standard 6 Assertion 2** All user devices are subject to anti-virus protections, while email services benefit from spam filtering and protection deployed at the corporate gateway. **Data Security Standard 9 Assertion 3** The organisation has a technology solution or service that prevents users from accessing potentially malicious websites, reducing the risk of the organisation's infrastructure being infected with malware. This could include the National Centre for Cyber Security's free DNS service.
Security update management Ensure that devices and software are not vulnerable to known security issues for which fixes are available.	**Data Security Standard 6 Assertion 3** Known vulnerabilities are based on advice from CareCERT, and lessons are learned from previous incidents and near misses. **Data Security Standard 8 Assertion 3** Supported systems are kept up-to-date with the latest security patches.

At their core, both the Cyber Essentials Scheme and the DSP Toolkit seek to secure data in similar ways. HOWEVER, the DSP Toolkit's detailed Independent Assessment Framework goes into far greater depth to guide NHS trusts more precisely.

While both require independent third-party audits to prove governance over data security and privacy controls, the DSP Toolkit also suggests that NHS trusts collect, aggregate, and review logs as part of the audit requirements.

CENTRALISED LOG MANAGEMENT: THE VISIBILITY TO SECURE DATA. THE DOCUMENTATION TO PROVE COMPLIANCE.

NHS trusts struggle with security and privacy because they need tools, but they often have limited budgets. Multi-functional solutions provide a way through the problem instead of trying to work around it.

Centralised log management is a solution to this problem. The right centralised log management solution can give the trust the visibility it needs into its security while also enabling other teams, such as operations and development.

As trusts build more robust cybersecurity and privacy programmes, they should consider centralised log management solutions that provide the security analytics necessary for gaining visibility into interconnected IT ecosystems. Instead of looking for a security-only tool, they can leverage centralised log management solutions as an overarching trust enabler. Ultimately, this gives them a way to monitor security and document compliance while giving other areas visibility into performance and availability.

SET THE RIGHT CONTROLS

When planning a log collection and management strategy, a trust should first set controls that align with the primary control groups:

- Identity and Access Management
- Configuration Management
- Information Security Programme Adoption
- Continuous Vulnerability Monitoring

COLLECT THE RIGHT DATA

Collecting too much data leaves the trust's security team overwhelmed while collecting too little information leaves the compliance team unable to provide the appropriate documentation for proving governance.

Once the trust establishes security controls based on its risk tolerance level, it needs to collect data that can alert the security team to potential threats and document its adherence to policies for the auditor.

Determining the most critical event logs to collect can be overwhelming, especially when the trust needs to meet multiple compliance requirements across more than one cybersecurity framework.

From a high level, trusts should, at minimum, collect data across the following six categories:

1. **Audit and Accountability**
   - User activity
   - Network connected systems and devices
   - Event source, date, user, timestamp, source address

2. **Identity and Access Management**
   - Device authentication and authorisation
   - User access to resources
   - Failed login attempts
   - Privileged access use
   - Remote logins
   - Application access

3 **Configuration and Change Management**
- Unauthorised changes
- Enforcement of access restrictions

4 **Continuous Controls Monitoring**
- System and application vulnerabilities
- Comparison of vulnerability scans
- Unauthorised traffic
- Risk-based prioritisation of vulnerabilities

5 **System Communications and Protection**
- Unauthorised inbound network traffic, including systems, users, and applications
- Unauthorised outbound network traffic, including systems, users, and applications

6 **Incident Detection and Response**
- Unauthorised commands
- Intrusion Detection Systems/Intrusion Prevention Systems data
- Incident scoring schema

CONTINUOUSLY MONITOR AND DOCUMENT CONTROLS' EFFECTIVENESS

Nearly every regulation and industry-standard require continuous controls monitoring. However, some trusts struggle as they still adhere to analogue point-in-time audit mentalities. Since malicious actors continuously evolve their threat methodologies, trusts need to monitor their controls' effectiveness continuously and document their processes as part of their proactive threat hunting process.

To protect against cyberattacks, trusts need to collect event log data and review it. As part of continuous monitoring, trusts should regularly review logs to detect anomalies indicating a potential cyber attack. For example, unsuccessful login reports can indicate a password

spray or attempted credential theft. Meanwhile, unauthorised software installation might mean malware executing on a device.

Continuously monitoring controls, documenting anomalies, and remediating detected weaknesses creates a “security-first” approach to compliance. Cybersecurity professionals recognise that compliance is not equal to security, so they should focus on documenting their security work for better audit outcomes. When security is the primary focus, compliance often follows nearly effortlessly.

PROVE COMPLIANCE WITH INTERNAL CONTROLS

Auditors need documentation that proves the trust is following its policies. Although cybersecurity professionals may like to lay claim to the “trust but verify” mantra, auditors have been following that since before the internet.

Event log data enables more robust compliance by providing objective documentation that proves the trust follows its internal controls. For example, user activity and access exception data prove that the enterprise enforces the principle of least privilege or makes purposeful decisions when making emergency access exceptions.

USE IN FORENSICS

No matter how hard a trust works to protect itself from a cyberattack, it will likely experience a data security event. Most cybersecurity professionals agree that the days of “if an attack” are gone, and they now look to managing the “when an attack” occurs.

Event log data, if properly collected, can provide visibility into how an attacker infiltrated a trust’s systems, networks, devices, and software. For example, configuring network vulnerability scanning tools to detect and alert unauthorised wireless access points connected to a wired network can provide insight into when or how a cybercriminal remotely accessed the enterprise infrastructure.

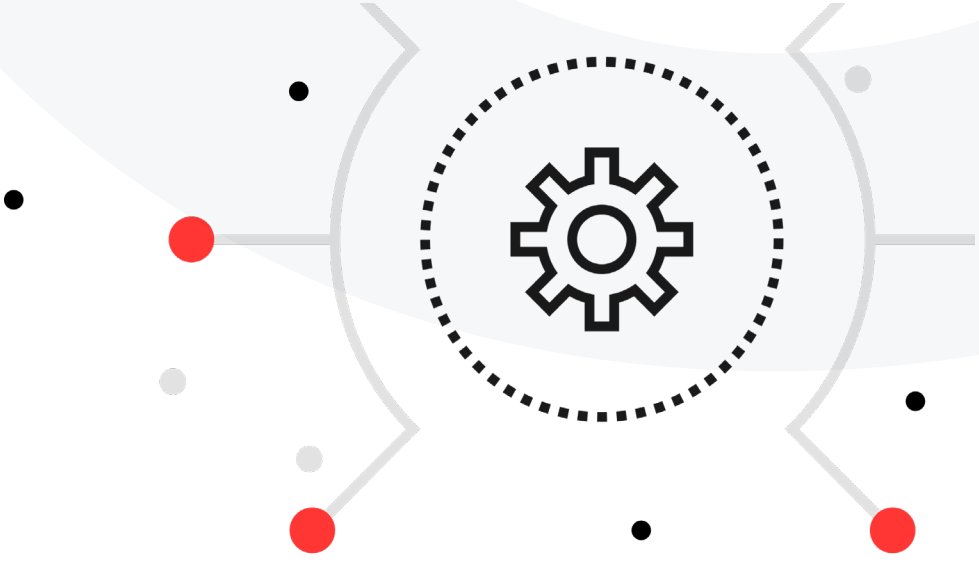
BREACH RESPONSE PROCESS

While the Cyber Essentials scheme does not indicate a breach response requirement, the DSP Toolkit, under Standard 6 Assertion 1 notes:

> **The organisation has a process/system for reporting resilience, network security, data security, and/or personal data breaches or near misses in line with its legal, NIS Directive, and DSP Toolkit reporting requirements.**

When trusts efficiently collect event log data, they can more rapidly determine the source of the data breach and reduce mean time to resolution. By carefully choosing how to aggregate and correlate log data, trusts can use automation more effectively, ultimately reducing the number of false positives, alert fatigue, and time taken to research the breach.

Additionally, log event collection and correlation enables trusts to document their breach response process and prove they complied with regulatory breach notification requirements.



GRAYLOG: SECURITY ANALYTICS FOR NHS TRUSTS

Graylog's centralised log management solution enables customers to document their compliance activities. With our centralised log management solution, compliance teams can collaborate, sharing and saving data in a single source of documentation. This reduces the operational costs associated with audits. Our Graylog Extended Log Format (GELF) standardises event log information. This solves divergent log formats' problems, making it easier for compliance teams to find patterns and reduce human error risk, leading to audit findings.

Graylog's solution syncs with an organisation's authoritative identity source, such as Active Directory or LDAP, to protect logs, ensuring appropriate rights and permissions. Additionally, we use encryption to protect log data, recognising that it often contains sensitive information.

With our Enterprise solution, compliance departments can create Teams. This functionality allows them to create and share dashboards. Using dashboards, the compliance team can create data searches that aggregate the information they need to collect to prove compliance. Within the dashboard, they can create charts and graphs, making review easier for the auditors.

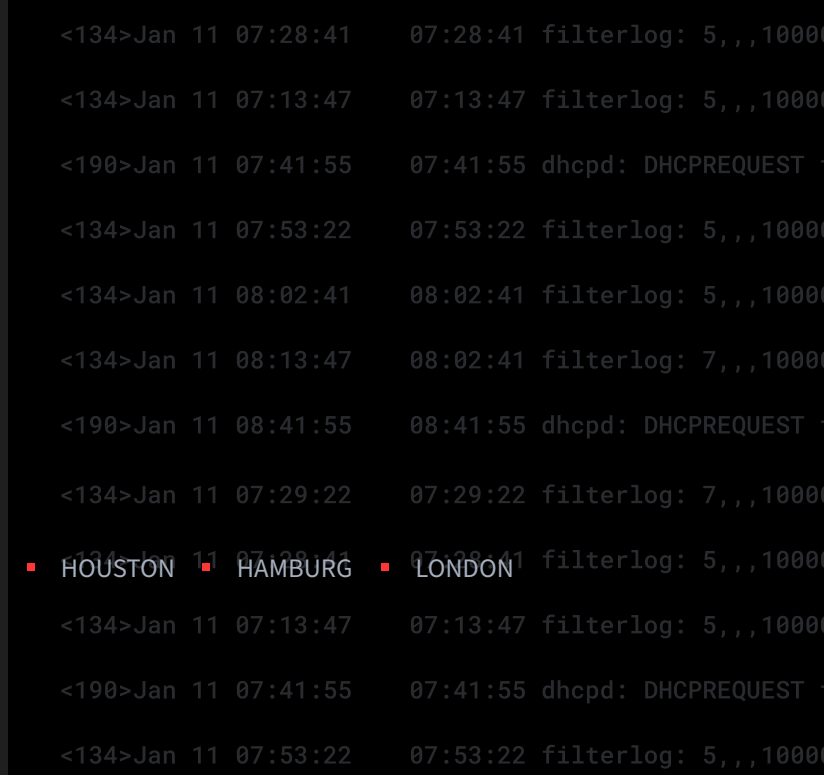
ABOUT GRAYLOG

Log management done right. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning centralised log management solution built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog enables hundreds of thousands of users to explore their data every day to solve security, compliance, operational, and application development issues.

graylog

www.graylog.org
info@graylog.com

1301 Fannin Street, Suite 2140
Houston, TX 77002



graylog

www.graylog.org ▪ HOUSTON ▪ HAMBURG ▪ LONDON