

APRIL 2026

MALAIKA WADDELL

SOLD ON DATA;

WHAT THE FDP CAN TEACH US
ABOUT GETTING PRIVATE SECTOR



Public dissatisfaction with the contract resulting in public demonstrations. Figure

1: Photo by TJ Chuah / Medact

Executive Summary:

In 2023, the UK's National Health Service (NHS) partnered with Palantir to create a unified data system; the Federated Data Platform (FDP) to reduce waiting lists, and increase operational efficiency. The FDP has invigorated a major debate about private partnerships in the NHS. The FDP contract represents a systemic failure in the NHS digital procurement processes. Without structural reform to transparency and governance frameworks, future NHS partnerships risk reproducing the same failures.

This policy brief evaluates the FDP within broader digital innovation efforts to improve efficiency and performance within the national public healthcare sector. Our analysis considers the contract's rationale, and evaluates dominant critiques against the FDP. To address these challenges, this report recommends implementing three major policy measures: 1) improving transparency in procurement phases, 2) ensuring structural diversification and local co-design, and 3) enforcing public interest safeguards. The implementation of these measures will improve efficient collaborations between the NHS and the private sector, increasing the likelihood of desired health outcomes through digital modernisation initiatives.



Public dissatisfaction with the contract resulting in public demonstrations. Figure 2: Photo by Talia Woodin for Medact

Introduction:

The solidaristic character of the NHS makes it one of the most trusted public institutions in the UK (Horn & Kerasidou, 2020). Given the widening funding gap which global healthcare bodies face alongside the introduction of data-driven technologies, private technology companies are increasingly accessing patient data through digitising and modernising healthcare systems. Following the successful 2022 pilot phase in Chelsea and Westminster Trust in London, £330 million was invested into collaborations with Palantir to modernise NHS England's healthcare delivery and efficiency (NHS England, 2023).

The contract has generated resistance, with public petitions garnering 200 000+ signatures against government collaborations with Palantir (Booth, 2026b). Palantir is a US-based data analytics firm specialising in artificial intelligence (AI) technologies, best known for its surveillance, border enforcement and military intervention work. Since the contract start date, the FDP's procurement, pilot phase testing and impact have all garnered significant critique.

This report addresses three primary problems in the FDP: 1) technological compatibility, 2) data sovereignty and 3) stakeholder satisfaction and trust. These concerns are inherent in public-private partnerships, and given the nature of NHS

patient data, future collaborations require a rigorous framework to avoid the levels of dissatisfaction with the FDP.

Background:

The NHS is a publicly funded healthcare provider for over 56 million people in the UK. There has been increased outsourcing from the NHS to the private sector since Margaret Thatcher's 1990 social care reforms (Goodair et al., 2024), and with the COVID-19 pandemic further increasing demands for privately funded initiatives (British Medical Association, 2020). Currently, Palantir provides surveillance and data support primarily to military and police agencies like the US' Immigration and Customs Enforcement (ICE). Palantir's collaboration with ICE generated the *Enhanced Leads Identification & Targeting for Enforcement* (ELITE) app, which ICE agents use to pinpoint people for deportation (Good Law Project, 2026a). The data which ELITE uses to locate individuals is generated by data from sensitive patient medical records (Good Law Project, 2026a). This raises a significant risk for the UK citizens and their healthcare data, given contracts with the UK's Ministry of Defence (MOD).

The FDP aims to streamline an integrated data system of patient information, enabling staff to efficiently manage waiting lists, appointments and diagnoses. FDP adoption has been slow, with only 123 out of 205 England hospital trusts adopting the system since 2023 (NHS England, 2026). Privately funded digitisation efforts in the NHS are not novel, and Palantir is certainly not the only technology company to be contracted for collaboration. One controversial effort was the 2016 NHS collaboration with AI-company DeepMind which accessed sensitive data for app development (Powles and Hodson, 2017). In 2025, the UK government announced plans to invest £10bn into technological/digital transformation for the NHS (Sollof, 2025). Successful digital transformation is critically dependent on public trust and cooperation, which cannot be generated simply through consent or the rational assessment of statistical information but also relies on the consensus that collaborations are being performed in service of the public good (Carter, Laurie and Dixon-Woods, 2015). Without trust, Britain's

health data infrastructure will remain underutilised or face repeated crises of legitimacy (Kerasidou and Kerasidou, 2023).

Problems:

Building and maintaining public trust in health care reforms is essential (Horn and Kerasidou, 2020). In 2013, the NHS launched care.data, an initiative for unifying data systems into a centralised database. This initiative was ultimately terminated in 2016, primarily due to poor data protection laws and communication (Presser et al., 2015).

Given the requirements for public trust outlined by Carter, Laurie and Dixon-Woods (2015), the distrust of the FDP is expected. Health Secretary Wes Streeting has refused to publicise briefing documents about the FDP's risks, expecting public trust through vague reassurances while refusing access to the facts (Good Law Project, 2026b). Recent investigations by the British Medical Journal (BMJ) demonstrate that even the pilot phase data is untrustworthy (Osborne, 2026).

This report evaluates the distrust of the FDP through three key concerns: technical compatibility, data privacy and sovereignty, and the lack of transparency to stakeholders during the pilot phase and rollout.

1) Technical capability

Research by BMJ evaluated how the contract secured with Palantir was reliant on an assessment of the pilot phase data. Through applying interrupted time series analysis (ITS), the BMJ found inconsistencies in the FDP pilot data (Osborne, 2026). The FDP at Chelsea and Westminster Trust was hailed for increasing theatre use and reducing inpatient elective surgery waiting lists by 28% (Osborne, 2026). But through the BMJ's ITS analysis, this is false attribution, and conflates correlation with causation (Osborne, 2026). NHS staff report that the technology is difficult to use, and does not match industry standard (Booth, 2026a). With slow adoption only 80 of the 123 NHS trusts live on the system have reported benefits (NHS England, 2026).

Palantir's UK representative Louis Mosley has stated that resistance to the FDP is politically motivated, "*putting ideology over patient care*" (Wright and Hayward, 2026). However, evidence shows that the FDP's technical capacity is not holding up to its promises (Booth, 2026a), and that Palantir secured the contract through misrepresentations of data (Osborne, 2026). The NHS published the contract with 417 out of 568 pages completely redacted, which prompted legal action by the Good Law Project (Good Law Project, 2024). The public has limited ability to find the truth as government restricts access to the foundational knowledge necessary for independent evaluation (Good Law Project, 2026b).

2) Data concerns

Frontier technologies require particularly high levels of transparency and communication given the novel risks and uncertainty of outcomes (Cheong, 2024). Palantir's historic data privacy controversies demonstrate lax data ownership, particularly in its 2016 NYPD contract, where Palantir refused to hand over readable versions of NYPD data to the police force, stating it would breach their own intellectual property (Price and Hockett, 2017). Palantir has been singled out by the humanitarian sector for its unregulated data protection (Dupraz-Dobias, 2025). The company's initial NHS collaboration was its first experience in healthcare, contracted during the COVID-19 pandemic (Foxglove and Doctors' Association UK, 2023). Palantir's inexperience with sensitive patient data raises questions as to what qualifies the company to work in the NHS.

The UK government is Palantir's second largest client, with government contracts totalling at least £670m (Cadwalladr, Young and Colbert, 2026). Given Palantir's networks in the MOD, NHS, and Britain's nuclear deterrence programme, there are significant concerns over potential misuses of confidential data. The handling of NHS data by foreign private companies inherently raise concerns (Agnew, 2026), and given Palantir's vested interests in defence and military intelligence, these are substantial. Despite Palantir's emphasis that data stored within internal NHS systems remains inaccessible to Palantir, legal architecture like the *Foreign*

Intelligence Surveillance Act in the US could “give law enforcement and intelligence the right to access data anywhere in the world if held by a US company” (Cadwalladr, Young and Colbert, 2026). In a recent debate about Palantir’s in the NHS, MP Martin Wrigley noted potential dependency issues which NHS England could face (Booth, 2026a). The outsourcing of this platform to an inexperienced foreign company inhibits the NHS’ capacity for data sovereignty and resilience, generating existential risks to the UK’s most valuable national assets – the confidential data of tens of millions of patients.

Centralised NHS data systems raise two key risks: data breach, and vendor lock-in. Centralised systems are increasingly demanded in development sectors to improve efficiency and transparency in big data infrastructures (Cheesman, 2017). But centralised systems increase the chances of vendor lock-in, as switching costs foreclose meaningful alternatives (Martins, Sahandi and Tian, 2016). This was anticipated with the FDP, with advisory groups warning that the public would need assurance the NHS would not be locked into a single supplier (Clark, 2023). While there is an argument for improved efficiency across siloed data systems, maintaining separate data systems decreases the risk of a breach compromising the infrastructure.

3) Stakeholder satisfaction and transparency:

Given alleged break clause activation in 2027, reports claim senior officials’ critiquing the FDP are being threatened for publicly criticising Palantir (Hughes, 2026). One NHS staff member reported being threatened by senior figures, stating this “creates compliance, not commitment” (Hughes, 2026). Independent or local alternatives for digitizing the NHS are being suppressed in efforts to push the ‘FDP-first’ approach set out in 2025-2026 NHS guidance (NHS England, 2025). This risks stunting initiatives which empower the NHS with data sovereignty, and raises the prospects of a vendor lock-in with a foreign company with strong military ties. The question of local development investment is significant given the scale of NHS care and output, as well as the confidential data itself.

Recommendations:

1) IMPROVING TRANSPARENCY

Potential improvements towards digital development are undermined by a lack of stakeholder trust in the FDP. The misrepresentation of its pilot phase data (Osborne, 2026) demonstrates the importance of transparency in process and sharing understandable data *before* implementation. The inherent safeguards of a rigorous pilot phase is an under-utilised phase that enables real-world capabilities for new systems. This should be enforced in future collaborations. Any transition from pilot phase to full integration should provide detailed rationale, allowing for independent validation of the rigour, independence and impartiality of the procurement.

End of pilot reports should be accessible to the patients whose data is being handled. These reports should be available in community languages and should be reviewed and published before decisions to extend/expand the contract are finalised. Stakeholders should be provided with opportunities to interrogate and edit reports before final implementation. The legal case against the FDP for its redacted pages was important (Good Law Project, 2024), but future collaborations should ensure contract transparency from the beginning. Future NHS digital partnerships should establish a public-facing, accessible Data Transparency Register which is updated periodically and covers which kinds of data are processed under these integrated data platforms.

Clearly demonstratable opt-in mechanisms for secondary data use need to be established (e.g. for research). There is a legitimate concern that opt-in frameworks could limit the scale of data available for wider application (Man et al., 2023). However the NHS' core principles place informed consent over operational efficiency, which must be reflected in digital partnership structures. The lessons from care.data are instructive, they show how a lack of transparency increases the risk of spreading misinformation, which can strengthen opposition, and increase the risk of costly delays and legal challenges. The failed care.data 2016 programme cost the NHS over £8 million and set back health data initiatives

(Shah, 2016).

2) UK-BASED COLLABORATION AND CO-CREATION

The FDP model has been critiqued for the manner in which it was procured and designed, a ‘top-down enforcement’ which suppressed alternatives in the name of efficiency (Hughes, 2026). Dependence on a single commercial firm for NHS data infrastructure increases the risk of vendor lock-in and limits UK data sovereignty. Future NHS digital procurement must encourage alternative solutions rather than defaulting to enterprise-scale private solutions.

A mandatory co-design phase must be introduced to future private-sector digital procurements, which include patient advisory channels, frontline clinical staff and community health organisations. This will help ensure designs are well adapted to NHS demands, and will empower stakeholders with ownership and influence over NHS digital development.

Given the NHS’ acutely sensitive data and concerns over data sovereignty, there should be stringent conditions that all data, including derived data, business processes, methods and other intellectual property be certified to be stored, transmitted and processed solely in the UK under strict cybersecurity protocols.

3) Enforceable public interest safeguards and safer pilot phases

Existing FDP governance frameworks contain extensive reporting obligations but insufficient mechanisms for triggered consequences for unmet targets. Future collaborations must replace voluntary reporting models with sustained Periodic Review Frameworks conducted by an independent body with established performance thresholds and break clauses in the case of unmet targets.

The NHS needs to define triggered consequences in the contract from the outset. These should include break clause conditions, contract suspension rights and a structured exit/transition protocol, alongside strategies to deal with issues like preventing vendor lock-in, intellectual property rights and the potential of data

breaches during transfers. Given the risks of frontier technologies, there should be clauses to manage unforeseen risks, which should grant overriding powers to force protective compliance through measures which allow the NHS to lock-down systems to ensure the safety and security of data and prevent abuse. In keeping with the transparency principles outlined above, the conditions under which these consequences should be enacted should be published *before* they are needed.

Given the risks, policy around NHS medical data should err on the side of prudence. Experimental and novel systems, particularly with frontline technologies like AI should be tested with siloed and small datasets which have stringent controls on confidentiality and security. These smaller scale and safe pilots, while complying with testing conditions like ITS to prevent false attribution, create evidence that will inform adoption into mainstream systems, and should be monitored and evaluated independently from the vendors and implementing parties deploying the pilot, to avoid bias and conflicts-of-interest. The anonymised and secure evidence will be shared in the aforementioned Data Transparency Register for stakeholders to review in real time.

Concluding Remarks:

The FDP has highlighted three central issues in NHS digital development initiatives; 1) technical capability, 2) data concerns and 3) stakeholder satisfaction and transparency. Through increased rigour and transparency of process, and stricter data sharing agreements during and after pilot phases, particularly in evidencing how procurement was won, similar platforms can be held to higher standards of public accountability. Future collaborations should be governed by pre-established evaluation criteria, independent secure oversight bodies and mandatory publicly accessible reporting at each stage. Embedding these recommendations and appropriate safeguards from the outset, alongside the high standards of data security, will increase the NHS' capacity for successful digital development.

Reference list:

Agnew, T. (2026) 'Sovereignty: A strategic imperative the NHS cannot ignore', Digital Health, 14 April. Available at: <https://www.digitalhealth.net/2026/04/sovereignty-a-strategic-imperative-the-nhs-cannot-ignore/>

Booth, R. (2026a). *Labour and Lib Dem MPs Demand 'Shameful' Palantir NHS Contract Be Scrapped*. [online] The Guardian. Available at: <https://www.theguardian.com/technology/2026/apr/16/labour-and-lib-dem-mps-demand-shameful-palantir-nhs-contract-be-scrapped>.

Booth, R. (2026b). *Thousands Call on UK Ministers to Cut Ties with US Tech Giant Palantir*. [online] The Guardian. Available at: <https://www.theguardian.com/technology/2026/apr/23/thousands-call-on-uk-ministers-to-cut-ties-with-us-tech-giant-palantir> [Accessed Apr. 2026].

British Medical Association (2020). *The Role of Private Outsourcing in the COVID-19 Response*. [online] BMA. British Medical Association. Available at: <https://www.bma.org.uk/media/2885/the-role-of-private-outsourcing-in-the-covid-19-response.pdf> [Accessed 2026].

Cadwalladr, C., Young, C. and Colbert, M. (2026). *Revealed: Palantir Deals with UK State Total at Least £670m – Including £15m Contract with Nuclear Weapons Agency*. [online] The Nerve. Available at: <https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley>.

Carter, P., Laurie, G.T. and Dixon-Woods, M. (2015). The Social Licence for research: Why care.data Ran into Trouble. *Journal of Medical Ethics*, 41(5), pp.404–409. doi:<https://doi.org/10.1136/medethics-2014-102374>.

Cheesman, M. (2017). Blockchain Technology: an Emergent, Political Infrastructure. *Anthropology of Infrastructure*. Available at:

<https://anthropologyofinfrastructure2017.wordpress.com/2017/01/20/blockchain-technology-an-emergent-political-infrastructure/> [Accessed 2026].

Cheong, B.C. (2024). Transparency and Accountability in AI systems: Safeguarding Wellbeing in the Age of Algorithmic decision-making. *Frontiers in Human Dynamics*, [online] 6. doi:<https://doi.org/10.3389/fhumd.2024.1421273>.

Clark, L. (2023). *NHS Watchdog Expresses Vendor lock-in Concerns over Federated Data Platform Deal*. [online] Theregister.com. Available at: https://www.theregister.com/2023/08/29/nhs_fdp_palantir_lockin/ [Accessed 2026].

Dupraz-Dobias, P. (2025). Donor crisis prompts rethink on humanitarian datapartnership rules. [online] Genevasolutions.news. Available at: <https://genevasolutions.news/peace-humanitarian/donor-crisis-prompts-a-rethink-on-rules-of-collaboration-for-humanitarian-data-partnerships>

Foxglove and Doctors' Association UK (2023). *The NHS Federated Data Platform and Palantir: 7 Key Risks*. [online] Foxglove, pp.4–17. Available at: https://www.foxglove.org.uk/wp-content/uploads/2023/06/2023_06_05-FINAL-The-NHS-Federated-Data-Platform-and-Palantir.pdf [Accessed 2026].

Good Law Project (2024). *NHS to Fill in the Blanks on Palantir's Heavily Redacted Contract | Good Law Project*. [online] Good Law Project. Available at: <https://goodlawproject.org/update/nhs-to-fill-in-the-blanks-on-palantirs-heavily-redacted-contract/> [Accessed Apr. 2026].

Good Law Project (2026a). *Palantir Uses Medical Records to Target People for ICE in the US – Will the UK Be next? | Good Law Project*. [online] Good Law Project. Available at: <https://goodlawproject.org/palantir-uses-medical-records-to-target-people-for-ice-in-the-us-will-the-uk-be-next/>.

Good Law Project (2026b). *Streeting Refuses to Publish Secret Palantir NHS Briefings | Good Law Project*. [online] Good Law Project. Available at:

<https://goodlawproject.org/streeting-refuses-to-publish-secret-palantir-nhs-briefings/> [Accessed 2026].

Goodair, B., McManus, A., Esposti, M.D. and Bach-Mortensen, A. (2024). How Outsourcing Has Contributed to England's Social Care Crisis. *BMJ*, 387, p.e080380. doi:<https://doi.org/10.1136/bmj-2024-080380>.

Horn, R. and Kerasidou, A. (2020). Sharing whilst caring: solidarity and public trust in a data-driven healthcare system. *BMC Medical Ethics*, 21(1). doi:<https://doi.org/10.1186/s12910-020-00553-8>.

Hughes, L. (2026). *Senior NHS officials warned staff over criticising rollout of Palantir platform*. [online] @FinancialTimes. Available at: <https://www.ft.com/content/ff701533-aa19-4ab0-80ff-70c9420f37d9?syn-25a6b1a6=1> [Accessed 16 Apr. 2026].

Kerasidou, A. and Kerasidou, C. (2023). Data-driven Research and healthcare: Public trust, Data Governance and the NHS. *BMC Medical Ethics*, 24(1). doi:<https://doi.org/10.1186/s12910-023-00922-z>.

Man, Y. de, Wieland-Jorna, Y., Torensma, B., Wit, K. de, Francke, A.L., Oosterveld-Vlug, M.G. and Verheij, R.A. (2023). Opt-In and Opt-Out Consent Procedures for the Reuse of Routinely Recorded Health Data in Scientific Research and Their Consequences for Consent Rate and Consent Bias: Systematic Review. *Journal of Medical Internet Research*, [online] 25(1), p.e42131. doi:<https://doi.org/10.2196/42131>.

Martins, J.O., Sahandi, R. and Tian, F. (2016). Critical Analysis of Vendor lock-in and Its Impact on Cloud Computing migration: a Business Perspective. *Journal of Cloud Computing*, 5(1), pp.1–18. doi:<https://doi.org/10.1186/s13677-016-0054-z>.

NHS England (2023). *NHS England - New NHS Software to Improve Care for Millions of Patients*. [online] NHS England. Available at:

<https://www.england.nhs.uk/2023/11/new-nhs-software-to-improve-care-for-millions-of-patients/>.

NHS England (2025). *2025/26 Priorities and Operational Planning Guidance*. [online] NHS England, NHS England, p.16. Available at: <https://www.england.nhs.uk/long-read/2025-26-priorities-and-operational-planning-guidance/> [Accessed 2026].

NHS England (2026). *NHS Federated Data Platform*. [online] NHS England. NHS England. Available at: <https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/impact/fdp-uptake-and-benefits/#impact> [Accessed 2026].

Osborne, R.M. (2026). Palantir: NHS Pilot's 'Success' Is Questioned as Second Figure at Major Trust Is Linked to the Tech Giant. *BMJ*, 393. doi:<https://doi.org/10.1136/bmj.s680>.

Powles, J. and Hodson, H. (2017). Google DeepMind and Healthcare in an Age of Algorithms. *Health and Technology*, [online] 7(4), pp.351–367. doi:<https://doi.org/10.1007/s12553-017-0179-1>.

Presser, L., Hruskova, M., Rowbottom, H. and Kancir, J. (2015). Care.data and Access to UK Health records: Patient Privacy and Public Trust. *Technology Science*. [online] Available at: <https://techscience.org/a/2015081103/> [Accessed 2026].

Price, M. and Hockett, E. (2017). Palantir Contract Dispute Exposes NYPD's Lack of Transparency | Brennan Center for Justice. [online] www.brennancenter.org. Available at: <https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency>.

Shah, S. (2016). *Scrapped NHS care.data Ballsup Cost Taxpayer Almost £8m*. [online] www.theregister.com. Available at:

https://www.theregister.com/2016/09/27/scrapped_nhs_care_data_cost_taxpayer_8_1m_pounds/.

Sollof, J. (2025). *Government to invest up to £10bn to bring NHS 'into the digital age'*. [online] Digital Health. Available at: <https://www.digitalhealth.net/2025/06/government-to-invest-up-to-10bn-to-bring-nhs-into-the-digital-age/>.

Wright, O. and Hayward, E. (2026). *Ministers Seek Advice on Scrapping Palantir NHS Data Contract*. [online] The Times. Available at: https://www.thetimes.com/uk/healthcare/article/palantir-data-contract-nhs-prrj8j9tm?gaa_at=eafs&gaa_n=AWetsqdAnx0cszPC_jvEKRz7a89gPupVYhdVyWOtZLUAWv5enruJD8bqlhO4NCGJs1l%3D&gaa_ts=69cb9528&gaa_sig=-h8bkz_7SkplHr_YVJcJZilg4eaOswNxo8ghCv58CMBJeCo4g54lG___m318D7qo4h1_6HuM-ASnMZO3lqZMVw%3D%3D [Accessed 2026].