Data & Policy (2026), 8: e50
doi:10.1017/dap.2026.10098

CAMBRIDGE UNIVERSITY PRESS

COMMENTARY

Performing trustworthiness: governance theatre versus governance maturity

Elizabeth Green and Felix Ritchie

University of the West of England Bristol Business School, UK
Corresponding author: Elizabeth Green; Email: elizabeth7.green@uwe.ac.uk

Received: 27 May 2026 UTC; **Revised:** 08 July 2026 UTC; **Accepted:** 03 August 2026 UTC

Keywords: data governance; Five Safes framework; governance maturity; statistical disclosure control; trusted research environments

Abbreviation: SDE, Secure Data Environments; TRE, Trusted Research Environments

Abstract

Universities, governments, and health research infrastructures increasingly invoke the language of "trusted," "secure," and "safe" research environments to legitimise access to sensitive data. While technical infrastructures such as Trusted Research Environments, Secure Data Environments, and cloud-based analytical platforms have expanded rapidly, equivalent growth in operational governance capability has not always followed. This article argues that contemporary research governance risks drifting towards "governance theatre": the performance of trustworthiness through visible technical controls, secure branding, and procedural symbolism while comparatively less attention is devoted to disclosure expertise, behavioural governance, independent oversight, and operational maturity. Using recent controversies surrounding the UK Biobank as an illustrative governance stress test rather than an isolated institutional failure, this article examines tensions emerging across contemporary research practices—including platformisation, global collaboration, artificial intelligence, code sharing, and increasingly complex data systems. Drawing on the five safes framework, this article argues that trustworthy governance cannot be reduced to technical infrastructure or formal compliance alone. Governance maturity depends upon layered socio-technical systems capable of managing disclosure risk, researcher behaviour, and organisational accountability across the full research life cycle. Moving beyond governance theatre will require greater investment in governance literacy, disclosure expertise, independent output review, and reflexive oversight capable of adapting to rapidly evolving systems.

Policy Significance Statement

This article argues that contemporary data governance policy has become overly focused on technical infrastructure and symbolic demonstrations of security, while comparatively less attention has been devoted to operational governance capability. Using the UK Biobank as an illustrative governance stress test, this article highlights the need for more mature, layered, and reflexive governance systems capable of responding to increasingly complex data-intensive research environments. This article recommends greater investment in governance literacy, disclosure expertise, independent output review, and behavioural governance across infrastructures providing data access. It further argues that governance frameworks such as the Five Safes should be treated as operational systems for managing socio-technical risk rather than as branding exercises or static compliance checklists. Strengthening public trust will depend upon governance maturity rather than technical infrastructure alone.

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

1. Introduction

Universities, health research infrastructures, and governments increasingly invoke the language of "trusted," "secure," and "safe" research environments to describe systems enabling access to sensitive data. The rapid expansion of TREs, SDEs, and cloud-based analytical platforms reflects growing recognition that detailed health and administrative data can generate substantial public benefit when used responsibly. Yet the growth of "secure" infrastructure has not always been matched by equivalent growth in governance capability.

Institutional discussions of trustworthiness have become increasingly focused upon technical infrastructure: secure logins, cloud environments, cybersecurity controls, and access management systems. These infrastructures are important, and they provide visible evidence that organisations appear to take data protection seriously. Governance vulnerabilities, however, frequently emerge not through external intrusion alone, but through interactions between technical systems, organisational processes, and ordinary human behaviour.

This distinction reflects a broader sociological problem identified by Meyer and Rowan (1977), who argued that organisational systems may function partly as institutional "myth and ceremony": visible demonstrations that an organisation is rational, responsible, and compliant, regardless of how deeply those structures shape everyday operational practice. Schneier's (2003) notion of "security theatre" similarly describes how highly visible security measures can function symbolically to reassure audiences while contributing comparatively little to substantive risk reduction. Within contemporary research governance, a comparable phenomenon is increasingly visible: governance theatre. Governance theatre emerges where institutional emphasis becomes concentrated upon performing trustworthiness through visible technical controls, secure branding, and procedural symbolism while comparatively less attention is devoted to operational governance capability, disclosure expertise, behavioural risk, and independent oversight.

Research environments increasingly involve global collaboration, cloud computation, linked administrative data, artificial intelligence, and large-scale genomic analysis. Academic systems strongly reward openness, reproducibility, and code sharing, creating tensions with the governance of confidential research data that require careful management. Governance systems originally designed around smaller-scale institutional research are therefore being asked to operate within increasingly complex sociotechnical environments. Although the governance challenges discussed have wider international relevance, this commentary is situated primarily within the United Kingdom, where Trusted Research Environments (TREs), Secure Data Environments (SDEs), and the Five Safes framework have become central to national policy for research using sensitive data.

The recent controversies surrounding the UK Biobank should therefore not be understood simply as isolated institutional failures or the actions of a few poorly behaved researchers. Rather, they function as a governance stress test exposing wider tensions emerging across contemporary data-intensive research. The significance of the case lies not simply in whether specific incidents occurred, but in what those incidents reveal about how trustworthiness is operationalised across modern research infrastructures.

2. UK Biobank as a governance stress test

UK Biobank provides an important illustrative case through which to examine these wider governance tensions. Established in 2003, UK Biobank provides approved researchers with access to detailed biomedical, genomic, imaging, and lifestyle data from ~500,000 participants. It has become central to thousands of studies spanning cancer, dementia, cardiovascular disease, diabetes, and ageing research, contributing substantially to genomics, artificial intelligence, and precision medicine research (UK Biobank, 2025a, 2025b). Central to UK Biobank's success has been a strong commitment to accessibility and scientific openness. UK Biobank has repeatedly argued that broad access to data is essential for accelerating scientific discovery and improving public health outcomes (BBC News, 2026a).

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

This philosophy reflects wider shifts across academia towards collaboration, computational scale, and data-intensive science, which can be seen in the proliferation of infrastructures providing access to health data for research (Goldacre and Morely, 2022).

UK Biobank has itself undergone a significant institutional transformation, evolving from a pilot study established principally through support from the Medical Research Council and Wellcome into a globally significant research infrastructure with a complex mixture of public, charitable, philanthropic, and commercial investment. Over time, the UK Biobank has developed substantial partnerships with pharmaceutical, biotechnology and technology companies, philanthropic and technology-sector investment, and infrastructure partnerships involving Amazon Web Services (UK Biobank, 2025b). These relationships are not inherently problematic, but they do complicate governance environments considerably by introducing competing pressures around openness, scientific acceleration, commercial value, and public accountability. Questions therefore emerge not simply around who may access data, but under what conditions, with what priorities, and with what temporal advantages. For example, UK Biobank's whole-genome sequencing initiatives granted consortium industry partners a period of exclusive access in return for substantial financial investment (UK Biobank, 2025c).

UK Biobank has faced increasing governance scrutiny concerning downstream data access, researcher vetting, commercial partnerships, international dissemination pathways, and the governance of highly detailed genomic data within increasingly complex research ecosystems. UK Biobank was investigated by the Information Commissioner's Office (ICO) for a data breach under the GDPR, case reference IC-491869-W4D0. The ICO concluded in April 2021 that "regulatory action [was] not required." However, substantial sections of the reasoning underpinning this conclusion were redacted under Section 44 of the Freedom of Information Act and the Data Protection Act 2018, limiting external scrutiny of the decision-making process.

These concerns intensified following the launch of UK Biobank's cloud-based Research Analysis Platform (UKB-RAP) in 2021, which adopted language strongly associated with Trusted Research Environment (TRE) governance, including secure access, controlled analysis, and participant protection (UK Biobank, 2025d). However, despite this transition towards platform-based infrastructure, downloadable participant-level data remained available under some access arrangements, raising questions regarding the extent to which governance protections remained operationally aligned with the rhetoric of secure research environments. The Guardian, a UK national newspaper, from 2023 onwards repeatedly indicated serious concerns over who had access to the data (The Guardian, 2023, 2024, 2025).

In April 2026, reports emerged that UK Biobank participant data had appeared for sale on a Chinese e-commerce platform, prompting international media attention, parliamentary scrutiny, and temporary suspension of parts of UK Biobank's access arrangements (BBC News, 2026b; UK Parliament Science, Innovation and Technology Committee, 2026). Parallel investigations also identified incidents in which researchers appeared to have inadvertently uploaded sensitive participant-level data to publicly accessible repositories and code-sharing platforms (The Guardian, 2026).

Critiques of UK Biobank governance within the privacy and data governance community have increasingly been taking a public stand. For example, Rocher (2026) documented concerns regarding downstream dissemination pathways and the discoverability of UK Biobank-linked data in public domains. Such critiques do not simply concern technical security failures, but broader questions surrounding governance assumptions, accountability, and the challenges of maintaining meaningful oversight within globally distributed and increasingly commercialised data ecosystems. The critiques and controversies should have acted as canaries in a coal mine regarding the UK Biobank's changing processes and protocols.

The 2026 incident was framed publicly as isolated examples of poor researcher behaviour or the actions of a few "bad apples" (BBC News, 2026c), but the issues exposed are far more systemic and extend well beyond the UK Biobank itself. Researchers are increasingly encouraged to share code, workflows, and outputs as markers of transparency and scientific quality. In such contexts, disclosure

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

vulnerabilities may emerge not primarily through malicious intent, but through routine research practices operating within governance systems insufficiently adapted to contemporary data-intensive science.

The significance of the UK Biobank controversy therefore lies not simply in the incidents themselves but in what they reveal about governance maturity across modern research infrastructures. The case highlights the risks that emerge when highly visible technical infrastructure and "secure" branding outpace the development of operational governance capability, including disclosure expertise, layered safeguards, governance literacy, and independent oversight.

The UK Biobank case also illustrates broader challenges associated with governing those infrastructures that are simultaneously internationally valuable, politically important, commercially connected, and highly dependent upon public trust. Institutions associated with major scientific success and national prestige may gradually become difficult to challenge, particularly where stakeholders fear criticism could damage wider research agendas or undermine public confidence. Under such conditions, institutional attention can become increasingly oriented toward reputational reassurance rather than reflexive oversight.

One particularly important tension concerns the relationship between platformisation and governance assumptions. Within mature TRE architectures, the separation between data access and data release functions as a central operational safeguard. Researchers analyse data within controlled environments while outputs leaving those environments undergo independent review. Allowing highly detailed participant-level data to leave the environment alters this balance substantially because protections then depend upon downstream researcher behaviour rather than layered institutional safeguards.

Historically, specialist secure research infrastructures were developed precisely because contractual agreements and researcher compliance alone were recognised as insufficient protections for highly detailed confidential data (Ritchie, 2017). Such systems were designed around assumptions that routine mistakes, misunderstandings, and behavioural limitations would inevitably occur over time. Layered safeguards (the "Five Safes") and independent output review existed not simply to prevent malicious misuse, but to create resilience against ordinary organisational vulnerabilities (Rocher and Morley, 2026).

The case also illustrates the wider challenges regulators face when overseeing rapidly evolving and globally distributed health-data infrastructures. As research ecosystems evolve through cloud computing, AI, and increasingly complex forms of data sharing, governance assumptions developed within earlier technological contexts may become outdated, particularly where oversight relies upon relatively static interpretations of compliance rather than more adaptive and principles-based approaches. This creates growing pressure for regulators and policymakers to develop more reflexive forms of oversight capable of responding to emerging sociotechnical risks.

The issue is particularly important because legitimacy within large-scale health data infrastructures is often recursively constructed. Institutions cite prior regulatory approval as evidence of trustworthiness, while regulators may simultaneously rely upon institutional assurances, technical safeguards, and evolving sector norms when assessing compliance. Over time, this can create situations where institutional safeguards appear validated even while important operational vulnerabilities remain weakly scrutinised and poorly understood. The issue is not whether organisations formally comply with governance frameworks, but whether existing oversight structures are themselves sufficiently equipped to interrogate complex sociotechnical research ecosystems.

These challenges become even more complex where research infrastructures operate across multiple legal jurisdictions. International collaboration is fundamental to contemporary biomedical research, but governance maturity must extend beyond technical access controls to encompass cross-jurisdictional accountability, regulatory interoperability, and effective oversight where researchers are located outside the United Kingdom. Recent UK Government guidance on safeguarding human genomic data explicitly recognises these challenges, recommending additional governance measures where access is provided to researchers in jurisdictions that do not provide UK GDPR-equivalent protections (Department of Health and Social Care, 2026). Although the guidance stops short of specifying how such governance should be operationalised in practice, its recognition of cross-jurisdictional oversight reinforces the need for more mature governance systems capable of managing increasingly international research systems.

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

The significance of UK Biobank lies not simply in the specific controversies themselves, but what they reveal about wider assumptions surrounding trustworthiness across academia. As public sector institutions increasingly adopt secure research infrastructures, there is a risk that institutional attention concentrates upon visible technical controls at the expense of disclosure literacy, behavioural governance, and operational oversight. UK Biobank therefore functions most usefully not as an exceptional institutional failure, but as a governance stress test exposing wider sector-wide tensions.

3. The institutional performance of trustworthiness: governance as infrastructure

A central weakness within many contemporary discussions of "secure" research is the tendency to treat governance primarily as a feature of infrastructure. Technical controls are often highly visible components of research systems, yet trustworthy governance depends equally upon less visible institutional capabilities including researcher training, disclosure expertise, independent oversight, operational procedures, and organisational culture (Green and Ritchie, 2023). Governance is not an administrative layer added around data access, but a core part of the infrastructure enabling sensitive data to be used safely and legitimately.

This multidimensional perspective is reflected within the Five Safes framework (Ritchie, 2017), originally developed to serve as the framework for the UK's first TRE at the Office for National Statistics in 2003. The Five Safes conceptualise governance as composed of safe projects, safe people, safe settings, safe data, and safe outputs. The framework explicitly refutes the idea that any single safeguard alone, in general, provides the required security. Rather, governance emerges through the interaction of multiple controls.

The framework also reflects a broader understanding that "secure" is not a binary state but a contextual and proportional concept. Effective governance operates across the "data access spectrum" (Ritchie and Kendal, 2024). At one end sit low-risk aggregate statistics and heavily anonymised public-use files requiring relatively few restrictions. At the other end sit highly detailed record-level data requiring substantially stronger procedural, organisational, and technical safeguards. Between these extremes exist multiple graduated forms of access involving varying combinations of anonymisation, researcher accreditation, licensing agreements, secure settings, and output review. Mature governance systems do not divide data into simply "open" or "secure"; they align safeguards proportionately across varying levels of sensitivity and disclosure risk.

In the Five Safes model, secure settings represent only one component of governance rather than governance itself. Safe people concerns whether researchers are appropriately trained and capable of handling sensitive data responsibly. Safe outputs recognises that disclosure risks may emerge not only from raw data, but also from tables, models, figures, synthetic data, and linked analytical products. Safe projects and safe data address the ethical and practical issues of making data available. The strength of the Five Safes lies in its recognition that trustworthy research requires these multiple interacting safeguards.

This layered approach also highlights the limitations of governance models relying heavily upon contractual compliance alone. Mechanisms such as data access agreements and material transfer agreements may bring comfort to legal teams, but they are comparatively weak behavioural safeguards. Researchers pay little attention to formal documents, but the issue is rarely deliberate misconduct. More commonly, misconduct reflects convenience, routine behaviour, and limited engagement with operating rules. Mature governance systems recognise that legal agreements alone cannot substitute for operational safeguards, meaningful governance literacy, and independent oversight.

In short, legal frameworks and technical infrastructures are highly visible and comparatively straightforward to communicate institutionally, and provide tangible demonstrations of responsible data stewardship. However, vulnerabilities emerge through interactions between elements of governance. For example, an organisation might impose cumbersome operating procedures, which researchers then ignore.

Consequently, mature governance requires more than technical or legal capabilities; other factors may include meaningful researcher training, independent output review processes, specialist disclosure

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

expertise, and governance cultures capable of balancing both data utility and confidentiality. In this sense, the defining characteristic of governance maturity is not the existence of a "secure platform" but the presence of a proportionate, layered, and reflexive system capable of managing risk across the entire research process.

For example, one of the least visible yet most important components of this governance infrastructure is output statistical disclosure control (OSDC): the discipline concerned with ensuring that statistical outputs based on confidential data do not inadvertently reveal that information (Derrick et al., 2024). For secure environments with very sensitive and detailed data, this risk is small but not negligible; small cell counts may reveal identifiable individuals within rare populations, for example. Disclosure risk is highly contextual and is not addressed through legal or technical processes but by training and approval processes. Hence, mature governance systems separate data access from data release, to provide an additional layer of protection against predictable human limitations and operational oversight.

4. Governance as theatre

UK Biobank explicitly states that it follows the Five Safes framework: (i) researchers are vetted and trained; (ii) projects must demonstrate public benefit; (iii) data are de-identified; (iv) analysis is conducted within the Research Analysis Platform; (v) and publications undergo review. However, the Five Safes is a framework to structure decision-making—not an instruction manual, a branding exercise, or a checklist.

Whether an organisation can formally map activities onto each of the Five Safes categories is therefore less important than how those safeguards operate in practice. At a sufficiently abstract level, many organisations handling sensitive data can plausibly claim alignment with the framework. The more significant issue is whether safeguards function as a mature, layered, and independently enforced governance system capable of managing disclosure risk and researcher behaviour operationally.

There are several projects formalising the Five Safes into operational guidelines, of which the SATRE (Standard Architecture for TREs; Cole et al., 2023) specification is most developed. SATRE is a principles-based approach to translating the Five Safes into concrete organisational, technical, and procedural expectations. Rather than simply asking whether an organisation claims to have "safe outputs" or "safe people," SATRE asks what demonstrable governance mechanisms exist in practice: independent output review procedures, auditing capability, researcher training standards, separation between access and release, disclosure controls, logging, accreditation pathways, governance oversight structures, and reproducible operational processes. Its 100-plus standards, assessed from "not applicable" to "fully implemented," provide a usable governance maturity framework.

The distinction between abstract alignment and practical maturity assessment matters because governance theatre frequently emerges precisely where conceptual frameworks are used for symbolic reassurance. Institutional language around "trusted" environments can create the appearance of comprehensive governance even where operational safeguards remain partial, inconsistent, or weakly enforced. The Five Safes was originally developed to avoid this reductionism by encouraging organisations to think holistically about how legal, technical, statistical, and behavioural protections interact (Green and Ritchie, 2023). Yet there remains the risk that the framework becomes something to hide behind, rather than serving as a tool for critically evaluating governance capability. Solutions such as SATRE are valuable precisely because they move discussion away from governance theatre based on symbolic claims of "trust," and towards the more difficult question of whether governance protections are meaningfully implemented, tested, and accountable in practice.

5. Behavioural governance and disclosure literacy

Much discussion surrounding "secure" or "trusted" research environments focuses primarily upon technical infrastructure. However, governance vulnerabilities frequently emerge through ordinary organisational behaviour rather than technical failure alone. Misunderstanding disclosure risks, oversharing

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

outputs, convenience-driven practices, competing institutional incentives, and limited governance literacy all shape how sensitive data are used operationally within research settings.

Consequently, trustworthy governance depends not only upon technical controls, but also upon behavioural governance: the design of systems, incentives, and institutional cultures shaping how researchers interact with sensitive data in practice (Green and Ritchie, 2023). This becomes particularly important within contemporary academic environments strongly oriented towards openness, collaboration, reproducibility, and rapid dissemination.

A longstanding issue within academia is that researchers often receive extensive training in ethics, research integrity, and legal compliance while receiving comparatively little education in operational disclosure risk or statistical disclosure control (Derrick et al., 2024). Researchers may complete postgraduate and doctoral training without ever formally encountering these. This creates a structural tension within contemporary research culture. Most governance vulnerabilities emerge not through malicious intent, but through routine organisational behaviour (Ritchie, 2021). Researchers operate within systems rewarding openness, publication, visibility, and collaboration. Under such conditions, disclosure risks may emerge through ordinary practices such as uploading supplementary materials, sharing code repositories, linking outputs across projects, or combining datasets in unanticipated ways. Governance systems designed around idealised researcher behaviour are therefore likely to be fragile.

This is why behavioural realism is central to governance maturity. Mature governance systems recognise that mistakes, misunderstandings, and routine human limitations are inevitable features of organisational life rather than exceptional failures of individual morality. The purpose of governance is therefore not simply to prevent malicious intrusion but to build resilience against predictable behavioural vulnerabilities. Secure settings alone cannot guarantee trustworthy research. Instead, governance depends upon layered systems involving researcher accreditation, training, behavioural expectations, auditing, and independent review processes.

6. Risks and culture

This recognition of where the real risks lie has important implications for organisational culture. Governance systems built primarily around suspicion and control may unintentionally discourage learning, openness, and early identification of problems. Fear-based governance cultures can create adversarial relationships between researchers and governance teams while simultaneously encouraging procedural compliance rather than meaningful understanding of disclosure risk (Ritchie, 2021; Green, 2024).

Institutions often operate somewhere between two broad governance orientations. Under *default-closed* governance, access is resisted unless safety can be conclusively demonstrated. Such systems prioritise institutional protection and minimisation of perceived risk, often producing highly defensive operational cultures focused primarily on restricting access, and are more likely to be principles-based. By contrast, *default-open* governance assumes that socially beneficial research should proceed wherever risks can be proportionately managed through layered safeguards and oversight, and is likely to rely on explicit operating rules (Green, 2024).

Default-open governance does not imply unrestricted access or weaker governance. Rather, it reflects a different governance philosophy: one recognising that governance should enable safe use rather than merely restrict use. Under this model, the objective is to design systems capable of managing behavioural and disclosure risks realistically across the research life cycle. Ritchie (2021) argues that this gives much more effective governance models, as all stakeholders have a common objective (making use effective), whereas in default-closed models, researchers and data owners have fundamentally incompatible objectives.

This distinction becomes increasingly significant as institutions adopt more complex analytical methods involving machine learning, linked administrative datasets, and distributed analysis models. Governance reliant on static rules or technical controls may be harder to adapt. Instead, effective

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

governance is more likely to depend upon institutional capability: disclosure expertise, governance literacy, and cultures capable of assessing risks fairly.

7. Concluding thoughts from theatre to governance maturity

The governance tensions exposed through contemporary data-intensive research ultimately point towards a wider challenge facing universities and research infrastructures: the growing gap between the performance of trustworthy governance and the operational capability required to sustain it in practice.

Moving beyond governance theatre requires recognising that trustworthy research is not created through technical infrastructure alone. Mature governance depends upon layered systems integrating technical controls, behavioural understanding, disclosure expertise, institutional culture, and independent oversight.

A priority is the development of governance literacy across academic research cultures. Current university training frequently focuses upon legal compliance, ethics applications, and data protection procedures while devoting comparatively little attention to wider governance. Researchers working with detailed health, administrative, and linked datasets increasingly require structured education in disclosure risk, safe outputs, and governance decision-making.

Second, there is a need to professionalise output review, in particular, and disclosure checking as recognised forms of specialist expertise. Output governance remains inconsistently implemented across many institutions despite functioning as a central safeguard within mature TRE systems. Effective output review requires contextual judgement, technical expertise, and institutional independence rather than purely procedural compliance.

Third, governance systems themselves must become more proportionate, layered, and reflexive. Mature governance does not divide data into simply "open" or "secure," nor assume that any single safeguard is sufficient in isolation. Instead, safeguards should operate proportionately across the data access spectrum while maintaining clear separation between data access and data release. Recent UK Government guidance on safeguarding human genomic data reinforces this direction by emphasising Secure Data Environments, layered governance, and proportionate safeguards for international access (Department of Health and Social Care, 2026).

Finally, institutions must move beyond governance cultures framing researchers primarily as threats to be controlled. Effective governance should not seek to eliminate data use, but to enable safe and trustworthy use through systems designed around realistic understandings of organisational behaviour.

The broader lesson emerging from the UK Biobank is not that sensitive data should not be used for research, or that openness itself is inherently problematic. Rather, it is that the rapid expansion of data-intensive science has outpaced the development of governance capability across significant parts of academia. The United Kingdom already possesses internationally recognised expertise in secure research governance through national statistical agencies, specialist data services, and TRE communities. The challenge now is ensuring that this expertise becomes embedded systematically across universities and research infrastructures before public trust is eroded further.

Ultimately, trustworthy governance should be understood not as technical or legal solutions, but as socio-technical governance systems grounded in operational legitimacy. Trust is not created by platforms alone. It is created by governance systems capable of managing disclosure risk, researcher behaviour, and institutional accountability through layered safeguards operating across the full research life cycle.

Data availability statement. No new data or code were generated as part of this commentary article.

Acknowledgements. The authors are grateful to colleagues within the trusted research and data governance community whose discussions and reflections informed the development of this commentary.

Author contribution. Conceptualization: E.G.; Formal analysis: E.G., F.R.; Investigation: E.G., F.R.; Methodology: E.G., F.R.; Project administration: E.G., F.R.; Writing—original draft: E.G.; Writing—review and editing: E.G., F.R. All authors have read and approved the final manuscript.

Competing interests. The authors declare no competing interests.

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.

References

BBC News (2026a) UK Biobank Researchers Defend Broad Data Access as Critical to Medical Discovery. *BBC News.*

BBC News (2026b) *UK Biobank Health Data Found for Sale Online. BBC News.*

BBC News (2026c) Biobank Data Incident Caused by "a Few Bad Apples", Boss Says. *BBC News*, 16 May.

Cole C, **Sood H**, **Oldfield K**, **Craddock M**, **Swanepoel N**, **Coleman S**, **O'Reilly M**, **Kerr D**, **O'Donovan C**, **Hetherington J and Madge J** (2023) SATRE: Standardised Architecture for Trusted Research Environments. [Computer software]. Zenodo. https://doi.org/10.5281/zenodo.21512203 (Accessed: 25 August 2026).

Department of Health and Social Care (2026) *Safeguarding UK Human Genomic Data*. London: Department of Health and Social Care. Available at https://www.gov.uk/government/publications/safeguarding-uk-human-genomic-data (Accessed: 25 August 2026).

Derrick B, **Green ER**, **Smith J F and White P** (2024) The inadvertently revealing statistic: A systemic gap in statistical training? *Significance 21*(1), 24–27. https://doi.org/10.1093/jrssig/qmae009.

Goldacre B and Morely J (2022) Better, Broader, Safer: Using Health Data for Research and Analysis. A Review Commissioned by the Secretary of State for Health and Social Care. [online]. Available at https://assets.publishing.service.gov.uk/media/624ea0ade90e072a014d508a/goldacre-review-using-health-data-for-research-and-analysis.pdf (Accessed: 25 August 2026).

Green E (2024) *Data Governance Mastery.* DPhil thesis.

Green E and Ritchie F (2023) The present and future of the five safes framework. *Journal of Privacy and Confidentiality 13*(2). https://doi.org/10.29012/jpc.831.

Information Commissioner's Office (ICO) (2026) IC-491869-W4D0. Disclosure log, 7 April. Available at ICO disclosure log entry (Accessed: 25 August 2026).

Meyer JW and Rowan B (1977) Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology 83*(2), 340–363. https://doi.org/10.1086/226550.

Ritchie F (2017) The "Five Safes": A Framework for Planning, Designing and Evaluating Data Access Solutions. *Data and Policy*

Ritchie F (2021) Microdata access and privacy: What have we learned over twenty years?. *Journal of Privacy and Confidentiality 11*(1). https://doi.org/10.29012/jpc.766.

Ritchie F and Kendal C (2024) The Data Access Spectrum. *Future Data Services Briefing note* 6. Available at https://uwe-repository.worktribe.com/output/13507443 (Accessed: 25 August 2026).

Rocher L (2026) *UK Biobank Takedown Notices.* Available at biobank.rocher.lc (Accessed: 25 August 2026).

Rocher L and Morley J (2026) Protecting health data at UK Biobank. *BMJ 393*. https://doi.org/10.1136/bmj.s660.

Schneier B (2003) *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus Books.

The Guardian (2023) Private UK Health Data Donated for Medical Research Shared with Insurance Companies. *The Guardian*, 12 November. Available at The Guardian article (Accessed: 25 August 2026).

The Guardian (2024) Concerns Raised Over Access to UK Biobank Data after "Race Scientists" Claims. *The Guardian*, 25 October. Available at The Guardian article https://www.theguardian.com/science/2024/oct/25/concerns-raised-access-uk-biobank-data-race-scientists-claims (Accessed: 25 August 2026).

The Guardian (2025) Revealed: Chinese Researchers Accessed Half a Million UK GP Records. *The Guardian*, 15 April. Available at The Guardian article https://www.theguardian.com/technology/2025/apr/15/revealed-chinese-researchers-access-half-a-million-uk-gp-records (Accessed 25 August 2026)

The Guardian (2026) *Confidential Health Records from UK Biobank Project Exposed Online. The Guardian*. https://www.theguardian.com/science/2026/mar/14/confidential-health-records-exposed-online-uk-biobank (Accessed 25 August 2026).

UK Biobank (2025a) Who We Are. Available at UK Biobank – Who we are (accessed 18 May 2026).

UK Biobank (2025b) Major Achievements. Available at UK Biobank – Major achievements (accessed 18 May 2026).

UK Biobank (2025c) World's Largest Genetic Project Opens the Door to New Era for Treatments and Cures – UK Biobank's Major Milestone. Available at UK Biobank news article (accessed 18 May 2026).

UK Biobank (2025d) Research Analysis Platform (UKB-RAP). Available at UK Biobank – Research Analysis Platform (UKB-RAP) (accessed 18 May 2026).

UK Parliament Science, Innovation and Technology Committee (2026) Biobank Data Leak: Committee Responds. Available at UK Parliament Committee Response (accessed 18 May 2026).

Cite this article: Green E and Ritchie F (2026). Performing trustworthiness: governance theatre versus governance maturity. *Data & Policy*, 8: e50. doi:10.1017/dap.2026.10098

Downloaded from https://www.cambridge.org/core. 17 Nov 2026 at 15:31:35, subject to the Cambridge Core terms of use.