IET response to the data access policy update consultation

About the Institution of Engineering and Technology (IET)

The IET is a trusted adviser of independent, impartial, evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community, with over 155,000 members worldwide in 148 countries. Our strength is working collaboratively with government, industry and academia to engineer solutions for our most significant societal challenges. Professional guidance, especially across all technological sectors, is critical to good policy-making.

Executive summary

1. **Enhanced Data Security and Privacy Measures**

   State-of-the-art cybersecurity measures, compliance with international standards, ongoing audits, and privacy-enhancing technologies are crucial for robust data security and privacy in Secure Data Environments (SDEs).

2. **Comprehensive Data Governance**

   Establishing clear, objective criteria for user access, an adaptive governance framework, and implementing data stewards and conflict resolution mechanisms can ensure robust governance and prevent potential misuse.

3. **Transparency and Accountability**

   Regularly publishing detailed reports on data access and usage, maintaining comprehensive audit trails, and promptly disclosing any data breaches can enhance transparency and accountability.

4. **Regular Public Engagement and User Education**

   Regular dialogue with the public, showcasing success stories, and mandatory training on data ethics, privacy, and security for approved users can enhance understanding, foster trust, and prevent accidental data misuse.

5. **Transparency and Accountability: Simplifying Data Policies and Defining Roles for Public Assurance**

   Making data policies easily understandable and clearly defining the roles and responsibilities of all parties involved can make the system more accessible, promote a culture of accountability, and reassure the public of the integrity of the system.

Introduction

The IET is encouraged by the NHS and the DHSC's commitment to increasing health and social care data application. They plan to adopt a 'data access by default' model bolstered by the initiation of Secure Data Environments (SDEs). As staunch supporters of the intelligent application of data and technology to enhance societal wellbeing, we see that the proposed benefits concerning data security, transparency, and expedited research perfectly align with our mission.

Previously, The IET published a report entitled 'Artificial Intelligence and Ageing - Machine Learning for Human Health and Longevity.' This report was highlighted in the House of Commons when an MP cited the report's recommendation to establish a National Institute for AI and Ageing to the Minister for Health and Secondary Care during a minister's questions session. Furthermore, we published 'The Digital Advantage' report, outlining our stance on the digital transformation of the NHS and social care across England. This report identified and summarised the inherent challenges of achieving interoperability and analysed the progress to date through a series of case studies.

Understanding the intricate balancing act of ensuring data accessibility, data security, and maintaining public trust, we offer our perspectives and suggestions, structured under crucial thematic areas:

1. **Data Security and Privacy**

As a broad and diverse engineering community, we've observed significant developments in data security and privacy and understand these elements' crucial role in the context of NHS data. The commitment towards establishing SDEs is a step in the right direction. However, we propose further enhancements to bolster data security and privacy further:

i. **State-of-the-Art Cybersecurity Measures**
Techniques like homomorphic encryption provide additional security by allowing data processing whilst remaining encrypted. Furthermore, integrating artificial intelligence and machine learning could enhance the detection and mitigation of cybersecurity threats.

ii. **Privacy-Enhancing Technologies**
Technologies like Differential Privacy complement anonymisation and pseudonymisation, enhancing privacy whilst maintaining data utility, thereby minimising the risk of re-identification.

iii. **Compliance with International Standards**
Aligning with global cybersecurity standards such as ISO/IEC 27001 is critical. We urge going beyond mere compliance to seek certifications that validate and demonstrate a tangible commitment to data security.

iv. **Ongoing Auditing and Monitoring**
Given the rapid evolution of cybersecurity, continuous threat monitoring and regular audits of SDEs are essential for early vulnerability detection and quick remediation.

v. **Inbuilt Security**

We advocate for 'Security by Design', integrating security measures into the system from its inception rather than as afterthoughts. This would ensure fundamental data protection within the SDEs.

vi. **Data Protection Impact Assessments (DPIAs)**
Conducting regular DPIAs for all major system or operational changes within SDEs can proactively address potential privacy risks.

Such measures will provide robust protection against potential data breaches and cultivate public trust in the system – a factor that is as crucial as the security measures themselves for the success of the SDE initiative.

2. Data Governance

The IET comprehend the intricacies of data governance. The draft policy's intent to vest NHS organisations with data oversight within SDEs and access decision-making authority is commendable. However, we believe more attention is needed in certain areas to ensure robust governance and prevent potential misuse:

i. **Clear and Objective Criteria**
Comprehensive, objective criteria for user access determination are essential. These criteria should account for the purpose and scope of data request, potential benefits to healthcare, ethical and professional standards adherence, and data privacy assurance.

ii. **Transparent Decision-Making Process**
A well-documented, publicly accessible decision-making process can foster trust among stakeholders. The reasons for approvals or denials of access should be clear and transparent.

iii. **Adaptive Governance Framework**
The data governance framework should evolve with technology and accommodate changing data needs and emerging ethical and legal issues associated with data usage.

iv. **Data Stewards**
Consider introducing Data Stewards, who would ensure privacy protection, legal compliance, and data quality. Their role would be crucial in data governance and provide users a point of contact.

v. **Conflict Resolution Mechanism**
Implement a neutral, transparent, and timely resolution mechanism for disputes over data access decisions. This would ensure fairness and trust in the decision-making process.

vi. **Independent Auditing**
Regular independent audits can serve as an additional assurance layer, ensuring data governance aligns with policy directives and ethical standards. Auditing can also help identify and address any gaps proactively.

vii. **User Education and Accountability**

Make regular training on data ethics, privacy, and security mandatory for approved users to mitigate inadvertent misuse. Additionally, establish a transparent and defined process to hold users accountable for data misuse.

Implementing these measures can strengthen data governance by ensuring clarity, adaptability, and accountability, promoting responsible data usage and fostering trust among users and the public.

1. **Transparency:**

As a professional body representing a diverse international community, we recognise the critical importance of transparency as a foundational element for public trust. While we commend the draft proposal for acknowledging this factor, we propose some additional measures to enhance transparency in the management and utilisation of Secure Data Environments (SDEs):

i. **Policies in Layman's Terms**
Make policies on data access, storage, and usage available and easily understandable. Craft these policies in everyday language, avoiding technical jargon, and ensure accessibility in various languages and formats for inclusivity.

ii. **Regular Reports on Access and Usage**
Publicly release reports detailing data access, purposes of usage, and outcomes. A user-friendly portal could be employed to inform the public about data use.

iii. **Detailed Audit Trails**
Develop a robust system for maintaining comprehensive audit trails to enhance accountability and oversight. This system should log all data interactions, enabling swift identification and response to potential misuse or anomalies.

iv. **Prompt Disclosure of Data Breaches**
In the case of a data breach, it is essential to make a swift, comprehensive, and honest public disclosure. This disclosure should encompass the nature and scope of the breach, parties affected, actions taken, and future preventative measures.

v. **Clearly Defined Roles and Responsibilities**
Clearly delineate and communicate all parties' roles, responsibilities, and accountability. This promotes a culture of accountability and reassures the public of the system's integrity.

vi. **Regular Public Engagement**
Engage in regular dialogue with the public regarding SDE operations, achievements, challenges, and future plans through various platforms like open forums, Q&A sessions, webinars, or newsletters.

vii. **Showcasing Success Stories**
Illustrate the value of data sharing by showcasing real-world examples and case studies to help the public understand how their data contributes to healthcare improvement and innovation.

Transparency must be ingrained as a culture, not just a policy, throughout the entire data-handling process within SDEs. These measures would considerably enhance trust and foster a more positive relationship between the NHS, data users, and the public.

Conclusion

In conclusion, initiating Secure Data Environments (SDEs) by the NHS and the DHSC is an encouraging step towards a future where data and technology are intelligently leveraged to

enhance health and social care. As highlighted in our response, significant opportunities exist to strengthen further the approach towards data security, governance, and transparency.

Incorporating advanced cybersecurity measures, privacy-enhancing technologies, comprehensive auditing and monitoring systems, and an 'inbuilt security' approach can provide robust data protection. This should be accompanied by conducting regular Data Protection Impact Assessments (DPIAs) to manage potential privacy risks proactively. Moreover, a well-defined data governance structure, complete with clear criteria for access, transparency in decision-making, data stewards, a conflict resolution mechanism, independent auditing, and a robust framework for user education and accountability, can ensure the responsible use of data.

Transparency also plays a pivotal role in nurturing trust among the public. Providing policies in everyday language, regular reports on data access and usage, maintaining detailed audit trails, and being prompt and transparent in case of data breaches is crucial. Moreover, frequent public engagement and showcasing success stories can help build a positive perception of data sharing.

Implementing these measures would not only help maximise the potential benefits of SDEs but also ensure the protection of individual privacy and foster public trust. A thoughtful and proactive approach towards data security, governance, and transparency is critical to harnessing the transformative potential of health and social care data. The IET, as a global professional body, is committed to supporting this evolution and looks forward to seeing the positive impact of such initiatives on our society.
.

For further information, please contact policy@theiet.org