Applications of privacy-enhancing technology to data sharing at a global pharmaceutical company

Received: 28th April, 2020

Stephen Bamford
Head of Clinical Data Standards & Transparency, The Janssen Pharmaceutical Companies of Johnson & Johnson, UK

Stephen Bamford is the Head of Clinical Data Standards & Transparency at the Janssen Pharmaceutical Companies of Johnson & Johnson. Stephen has been a member of the Janssen team since 2016 and has helped to implement and support a number of data-sharing initiatives during this time. He has over 25 years of experience in management of clinical trials and research data with pharmaceutical, life science and research organisations. In 2004, Stephen founded the PHUSE organisation. Since inception, he has driven, and continues to drive, PHUSE, which now has over 10,000 global members. PHUSE runs over 25 well-attended events globally each year, including a data innovation symposium in partnership with the Food and Drug Administration.

Janssen Research & Development, 50-100 Holmers Farm Way, High Wycombe, HP12 4DP, UK
Tel: +44 1491 567351; E-mail: sbamford@ITS.JNJ.com

Abstract Janssen has been at the forefront of the recent pharmaceutical industry trend towards more transparency and sharing of clinical trials data, committing early on to make its data available for both internal and external innovation. Janssen is also committed to protecting patient privacy and giving individuals a voice on how their data is used and disclosed. This paper outlines Janssen's data-sharing initiatives and describes how it is using leading-edge privacy-enhancing technologies (PETs) to mitigate privacy risks and find the right balance between innovation and privacy.

KEYWORDS: privacy-enhancing technologies, data sharing, transparency, pharmaceutical industry, open data, clinical trial data

INTRODUCTION

There has been a strong trend in recent years towards more transparency and sharing of data by the pharmaceutical industry. Pharmaceutical companies and regulators have made a push for more open sharing of clinical trials data, necessitating a greater focus on responsible methods by which to share data with researchers, patients and the public.[1] Secondary use of clinical trial data, beyond the purposes for which the data was originally collected, has the potential to enhance the safety and efficacy of new treatments, encourage and accelerate innovation, and reduce research and development costs.[2] As a result, secondary use benefits patients, researchers and the general public in addition to the pharmaceutical industry.

But secondary use and sharing of data must be done in a responsible manner that safeguards the privacy of data subjects.[3] Ethical guidelines indicate that the autonomy of individuals must be respected and that both the benefits and burdens of research be balanced and fairly distributed.[4] Moreover, the current regulatory climate is trending towards an increased emphasis on individuals' rights and privacy safeguards. When implementing mechanisms for using and sharing data for secondary purposes, organisations must take into account many,

sometimes competing, considerations, such as data governance requirements, privacy risks, data utility, regulatory compliance and rapid innovation. A structured decision-making process is needed to ensure decisions around data use and sharing are made in an ethical, legally appropriate and replicable manner.

Generally, data-sharing mechanisms involve varying degrees of restriction. At one extreme, data could be made publicly available with no access restrictions. For example, data could be posted on a website for anyone to access without restrictions placed on its use or disclosure. Conversely, data could be disclosed through a controlled-access mechanism. There are many ways in which this could be operationalised, but it would typically entail a data use agreement (DUA) with the recipient[5] of the data stipulating how the data is to be used and the privacy and security protections required to safeguard it. There would also be greater restrictions placed on who could access the data through a controlled-access mechanism (ie qualified researchers could access it, but not members of the general public).

Although the industry as a whole is moving in the direction of more open sharing of data, data-sharing strategies and approaches to privacy protection vary greatly between companies. The mechanisms employed will differ based on each company's requirements and priorities as well as their risk tolerance.

In this paper, the authors focus on secondary use and sharing of structured individual patient clinical trial data (IPD). Although there may be some overlap in the privacy-enhancing technologies (PETs) used for structured IPD and other forms of data (eg free text, images etc), this discussion will be limited only to data-sharing initiatives and PETs for structured IPD.

DATA-SHARING INITIATIVES

Janssen has committed to making much of their clinical trial data available for both internal and external innovation. It has several data-sharing initiatives underway, including participating in the Yale Open Data Access (YODA) Project,[6] Project Data Sphere,[7] TransCelerate Biopharma's data-sharing initiatives[8] and direct collaborations with the research community, in addition to disclosures required by health authorities such as the European Medicines Agency (EMA)[9] and Health Canada.[10]

For sharing clinical trial data, there are two mechanisms that can be used: microdata releases and access via a portal or platform.[11] Under the first mechanism, individual participant records (microdata) are released to the data recipient. Under the second, access to the data is provided through a controlled-access platform. This option does not allow the data recipient to download the data; all analysis is performed within the data-sharing platform. The platform provides access to common statistical and graphing software to allow performance of the necessary analyses wholly within the portal.[12] The results are then downloaded (verification may be required prior to download), but no individual-level data is allowed to leave the portal environment.

Janssen, like most companies today, uses and shares data both internally and externally for secondary purposes. Internal uses include purposes such as internal data science projects and software testing as well as research-related purposes (eg planning future clinical trials), while external secondary purposes are all research related. In all of these cases, the appropriate PETs and associated controls are applied. The application of PETs in various secondary use contexts will be discussed in more detail in the next section.

Janssen's external data-sharing initiatives take many shapes, as described earlier. Janssen shares data via the YODA Project established by Yale University in 2013.[13] Johnson & Johnson (and Janssen by extension) is the only healthcare company to

share data from across all of its product lines through the YODA Project platform.[14] The project's data-sharing model is a controlled-access model that requires preapproval, by the YODA team, of the proposed research prior to giving data access to qualified researchers. Researchers also must sign a YODA DUA, outlining restrictions on the use and disclosure of the data and the safeguards required to protect data subjects' privacy.[15] Researchers are obligated to publicly disseminate their research findings from studies accessing data via the YODA Project.[16] In Janssen's case, access to data is provided via a portal that allows researchers to access and analyse the data within a secure environment[17] (no downloading of data is permitted[18]).

There are also industry-based data-sharing initiatives led by TransCelerate and Project Data Sphere in which Janssen participates. DataCelerate is a data-sharing platform developed by TransCelerate BioPharma, a nonprofit organisation made up of a number of biopharmaceutical member companies (Janssen being a member).[19] This initiative was established to facilitate data sharing between pharmaceutical companies with the goal of accelerating clinical research.[20] The platform provides access to preclinical toxicology data and data from TransCelerate's Placebo and Standard of Care initiative. Participating companies may download the data after agreeing to a data-sharing agreement outlining the conditions on its use and the privacy and security controls needed to safeguard the data. Each organisation maintains control of the data they share with the ability to approve or deny requests for access. Data shared through this initiative has been used to improve study design and inform clinical analyses.[21]

Project Data Sphere is a data-sharing platform housing data from late-stage cancer clinical trials.[22] Researchers from industry, healthcare and academia and independent researchers without an affiliation can apply to become authorised users. Users must agree to the terms of use for the data prior to getting access. Greater access to cancer trial data aims to increase the efficiency of research and accelerate research discoveries.[23] Similar to the YODA Project, access to data is provided via a secure platform, which also contains statistical tools for analysing the data. Analysis can then take place completely within the secure platform environment without the need for researchers to download the data.[24]

Janssen also works directly in collaboration with researchers to provide access to data. There have been cases in which the data or software required to explore a certain line of inquiry was not available through one of the initiatives discussed earlier, and a direct collaboration was arranged with Janssen to allow researchers access to the data.[25]

Regardless of the mechanism for sharing, privacy-preserving technologies play a role in any responsible secondary use and sharing of clinical trials data. Janssen applies PETs to the clinical trial data that is shared for secondary purposes. There is a strong leadership commitment within the company to protecting individual privacy and enabling innovation in a responsible manner that respects subjects' data rights.

PRIVACY-ENHANCING TECHNOLOGIES

PETs come in many shapes and sizes. One can think of PETs as a set of tools in a toolbox that can be employed based on the context and priorities of the user. Apart from the basic reduction of personal information that is legally required by health authorities for certain policy disclosures (eg European Medicines Agency policy on access to documents [EMA Policy 0043][26]), the main PETs in the Janssen toolbox are pseudonymisation, anonymisation and data synthesis.

In all cases where PETs enable the secondary use and sharing of data, the data is not then shared indiscriminately. The merit of a particular data use or research undertaking is always taken into consideration as well as the conditions of the consent provided by participants at the time of data collection. Oversight is needed to ensure that the data is used in an ethical and legally appropriate fashion. There is always a governance overlay even when PETs are applied.

'Pseudonymization' here refers to a method of removing or replacing direct identifiers (eg names, phone numbers, identification numbers etc) from a dataset but leaving in place data that could indirectly identify a person (often referred to as indirect or quasi-identifiers).[27] Indirect identifiers are pieces of information such as age, gender, ethnic origin and so on that could be used, in combination with other pieces of information, to identify individuals. The replacement of direct identifiers can be done through encryption of the values or by replacing them with random values. Although pseudonymised data does not directly identify individuals, it is considered to be personal information in most jurisdictions due to the risk posed by indirect identifiers and is, therefore, subject to the restrictions and requirements of applicable privacy laws. Although in some cases pseudonymisation may help to meet legislative obligations, it does not exempt the data from privacy regulations.[28]

Anonymisation, also called de-identification in some jurisdictions,[29] refers to techniques applied to personal information in order to minimise the risk posed by indirect identifiers found within the data. Under a risk-based anonymisation approach, data is determined to be anonymous as a result of both data transformations and additional technical and contractual controls that must be put in place. Fully anonymised data that meets the legal requirements of applicable privacy laws is not considered to be personal information and is no longer subject to the restrictions and requirements of those laws.

Generating synthetic data involves using the characteristics of an original dataset to produce a simulated dataset with a similar structure and statistical properties.[30] The process models the statistical distributions and structure of a clinical trial dataset. Using that model, synthetic data records are generated that are similar to the original data but do not link to actual individuals. This modelling must be done carefully because when there is overfitting of a model, the result is effectively replication of the original data. When data synthesis is performed in a manner that produces structurally similar but not identical data, the resulting synthetic data would not be personal information and, consequently, would not be subject to regulatory restrictions and requirements.[31]

THE APPLICATION OF PETS TO DATA SHARING

Janssen deploys PETs in different contexts depending on the priorities of the company and the use case at hand. Although certain PETs may be commonly used in certain contexts, companies do not necessarily deploy PETs in the same way in every data-sharing context. The choice of PETs is not universal and is dependent on criteria that may be specific to each company. In this way, PETs can be seen as a set of tools that can be deployed based on the priorities of the user. One company may deploy pseudonymisation in a given context, while another may choose to use anonymisation or a different PET for the same purpose based on its unique requirements and priorities.

An overarching principle guiding the implementation and use of PETs at Janssen is data minimisation. Data minimisation is a requirement of many global privacy regulations, such as the General Data Protection Regulation (GDPR)[32] in

	Weight	Rankings		
		GDPR Pseudonymization	Risk-Based De-identification	Data Synthesis
PRIVACY	0.45	3	1	1
PATIENT TRUST	0.40	2	2	1
OPERATIONAL COST	0.05	3	2	1
DATA UTILITY	0.10	1	2	2
SCORE		0	0.653	1

Figure 1: Illustration of a weighted ranking method for selecting of PETs
Note: GDPR, General Data Protection Regulation; PETS, privacy-enhancing technologies.

the European Union and the Health Insurance Portability and Accountability Act (HIPAA)[33] in the United States. The principle indicates that personal information being collected, used or disclosed should be 'limited to what is necessary in relation to the purposes for which they are processed'.[34] The use of PETs ensures that the principle of data minimisation can be operationalised in a way that both complies with privacy regulations and upholds the privacy rights of data subjects.

Criteria should be used for selecting a particular PET. A simple weighted ranking method can be used as illustrated in Figure 1. The weights (column) reflect the priority attached to the four criteria that Janssen uses: (a) the extent of privacy protection for the individual, (b) the utility of the data after it has been transformed by the PET, (c) maintaining patient trust and (d) the cost sensitivity of the organisation. The weights must add up to one. The weights Janssen uses emphasise privacy and patient trust as important criteria, and PETs that optimise on these criteria are favoured. The ranks in the table reflect how each of the PETs optimises each of the criteria. For example, a rank of one means that a particular PET better satisfies a criterion than a rank of two or three. The score is a normalised average rank that has a higher value, the greater a particular PET satisfies the four criteria. Based on this ordering, the decision flow illustrated in Figure 2 was devised.

Different pharmaceutical companies can assign a different set of weights that reflect their own business imperatives. But at a minimum, this process provides a mechanism to make decisions in a repeatable and transparent manner and to justify one's processes.

One can consider a number of examples. For internal purposes, such as software testing, a form of pseudonymisation may be used, which addresses the risk from direct identifiers while ensuring that there are no unique records in the dataset based on demographic information.[35] When pseudonymisation is used, it is applied in conjunction with privacy and security controls as required under the relevant legislation as pseudonymous data is still considered personal information. Pseudonymisation is used internally because there is greater control over who is using the data for what purposes and how it is being processed.

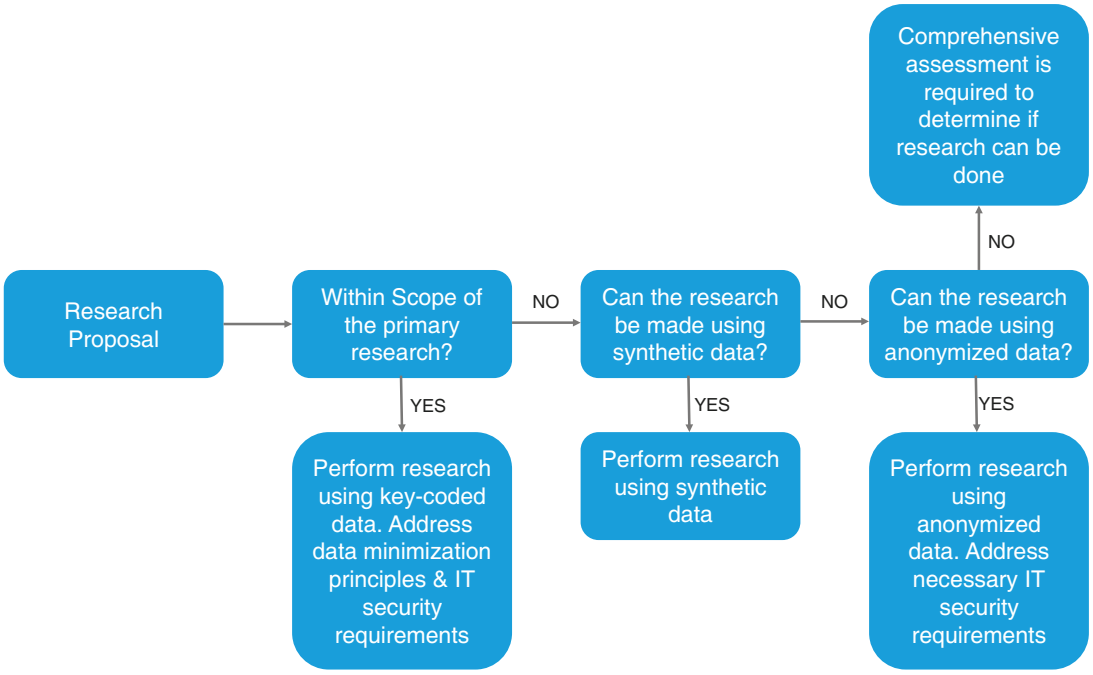

Figure 2: Decision-making process regarding internal data use for research purposes
IT, information technology.

Synthetic data may also be used for internal purposes, based on data requirements and other contextual factors. Fewer controls may be used with synthetic data as it would not be considered to be personal information. As mentioned earlier, the goal is always to use the minimum amount of personal information while maximising the utility of the resulting dataset. When data is released externally for secondary purposes, there is a lower degree of control over the 'who,' 'what' and 'how' of data processing. As such, the choice of PET will be different and will reflect the greater level of privacy protection required and any other controls that might be in place to ensure appropriate use. For example, for anonymised data, additional security and privacy controls are implemented by the data processor to ensure that the re-identification risks are low.

The internal decision-making process is illustrated in Figure 2. This shows the options considered when deciding on the type of data appropriate for a given purpose.

For secondary analyses that are not consistent with the consent provided by data subjects at the time of data collection, or otherwise deemed compatible under applicable law, anonymisation would be applied prior to use or sharing of the data. Just because de-identification may make certain transactions legal and possible, it may not always, however, be ethically appropriate to share said data. Synthetic data may also be used in this context when appropriate, depending on the particular requirements of the analysis. As illustrated in Figure 2, the use of synthetic data for research purposes is preferred whenever possible.

For external data sharing, the decision-making process would begin at the second step, as primary research only applies to internal purposes and pseudonymous data would generally not be shared externally. In the case of external data sharing, data synthesis and anonymisation are the preferred PETs. Data shared through the YODA Project is anonymised prior to

researchers being given access. Although Janssen provides access to data via a secure portal mechanism, the data being accessed is also anonymised to further protect data subjects' privacy. Data being shared through the DataCelerate and Project Data Sphere initiatives is also anonymised prior to release. For direct collaborations with researchers, data anonymisation or the generation of synthetic data is the preferred mechanism for responsibly sharing data. These technologies offer greater privacy protection for data being shared externally and ensure that the risk to patient privacy is minimal.

LESSONS LEARNED

There have been several lessons learned over the years about applying PETs in a large pharmaceutical company. Even for companies with a strong commitment to privacy protection, it can sometimes be a challenge to get buy-in for new privacy initiatives.

Rogers' Diffusion of Innovation Theory, which researchers have applied to the adoption of PETs,[36] indicates that the adoption of innovation depends in part upon the attitudes of management in regards to change.[37] If management is resistant to change, they will likely not be open to the changes that adopting a new technology will involve. Furthermore, enhancing emphasis on privacy protection requires a change in perspective within the organisation in regard to data ownership, data use and data management. This can be difficult to sell to a management team that is not open to change.

Technology users may also be a barrier to adoption. Introducing a new technology involves changes to the way people work, and this can be difficult for some to accept. According to a recent review by the Canadian Federal Privacy Commissioner's Office, users may be resistant to PETs that are overly complex and/or not user friendly.[38] Users may also not trust new technologies that have had limited practical application and are not 'tried and tested'.[39]

Fortunately, this is not a process that requires a full commitment upfront; PETs can be implemented in stages over time. Establishing initial short- to medium-term goals can help to slowly bring management on side and change perspectives. For example, one short/medium aim could be to build up a large library of studies that will allow multiple and different uses of clinical trials data. When the value of the data is demonstrated in this way, and the use of PETs to unlock that value is highlighted, attitudes can be changed and support increased for these initiatives. An organisation can then transition to longer-term data-sharing goals and select the most effective PETs to help realise those goals.

Another organisational factor Rogers indicates could have an impact on the adoption of innovation is internal relatedness.[40] Internal relatedness is the degree to which internal members and/or divisions within an organisation are interrelated.[41] This interrelation can be a critical factor in the adoption of PETs. Members from different departments will likely need to work together in order to implement such a technology, and some may never have worked together before. With a low level of interrelation between departments, collaboration on PET implementation may be difficult and organisations may rather not move forwards with an implementation that risks failure. Increasing the extent of internal relatedness between departments, through relationship building, for example, is key to ensure they can effectively work together for a successful implementation.

It is also important to note that when an organisation is bringing in a new data-sharing initiative and associated PETs, a support structure is required to track and record data-sharing requests and report on data usage. This becomes important as data sharing scales up, with many datasets

and numerous data requesters. Some level of tracking and reporting of secondary uses of patient data is required in order to fulfil the obligations of the various privacy regulations, although the level of tracking and reporting necessary may differ between jurisdictions. Tools supporting the large-scale implementation of PETs can be useful in this regard, and there are such tools available that track data usage, provide reports on data releases and associated privacy and security safeguards, and present other functions that may be useful in demonstrating compliance.

In addition to support meeting of regulatory obligations, tracking is important to be able to make the business case for investing in a data-sharing infrastructure and the required PETs. Evidence of data demand and utilisation becomes critical over time to sustain these investments.[42]

CONCLUSION

Following the recent trend towards more transparency and sharing of clinical trials data, Janssen has committed to making much of its clinical trial data available for both internal and external innovation. The data-sharing initiatives with which Janssen is involved, such as the YODA Project, Project Data Sphere and DataCelerate, are revolutionising the way in which clinical research is conducted to the benefit of researchers, the industry, patients and the public. But data sharing must be done in a responsible manner that respects the privacy of data subjects and honours the commitments made to clinical trial participants. This is where PETs come in, to enable innovation while ensuring that individual privacy is protected and the autonomy of research participants is respected.

The three main PETs used by Janssen for its data-sharing initiatives — pseudonymisation, anonymisation and data synthesis — are practically proven technologies that are being broadly applied across many industries in various different contexts to safeguard patient privacy. In conjunction with these PETs, and where necessary to manage privacy risks, additional privacy, security and contractual controls are put in place. The use of the PETs ensures that Janssen remains compliant with all applicable privacy regulations while allowing it to leverage data resources to uncover new insights and spawn innovation.

References and Notes

1. Phrma & EFPIA (2013) 'Principles for responsible clinical trial data sharing', available at: http://www.phrma.org/sites/default/files/pdf/PhRMAPrinciplesForResponsibleClinicalTrialDataSharing.pdf (accessed 7th November, 2019); TransCelerate Biopharma (2017a) 'De-identification and anonymization of individual patient data in clinical studies: A model approach', available at: http://www.transceleratebiopharmainc.com/wp-content/uploads/2015/04/TransCelerate-De-identification-and-Anonymization-of-Individual-Patient-Data-in-Clinical-Studies-V2.0.pdf (accessed 7th November, 2019); TransCelerate Biopharma (2017b) 'Protection of personal data in clinical documents: A model approach', available at: http://www.transceleratebiopharmainc.com/wp-content/uploads/2017/02/Protection-of-Personal-Data-in-Clinical-Documents.pdf (accessed 7th November, 2019).
2. Institute of Medicine (2015) 'Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk', IOM, Washington, DC.
3. The legal term 'data subject' is used in this paper to refer to a clinical trial participant from whom data was collected. The term 'data subject' is used in the European Union's General Data Protection Regulation (GDPR) to refer to a 'natural person' to whom the data relates (see GDPR Article 4: Definitions). 'Subject' is also a term used in research to refer to 'research subjects' or 'clinical trial subjects'; the industry-preferred term is, however, 'participant' rather than 'subject'.
4. U.S. Department of Health and Human Services and Food and Drug Administration (2016) 'ICH Harmonized Guideline: Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice ICH E6(R2): ICH Consensus Guideline', https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf (accessed 24th May, 2020); Office for Human Research Protections (1979) 'The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, "The Belmont Report"', Department

of Health, Education, and Welfare, available at: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html (accessed 2nd February, 2017).
5. Article 4(9)(1) of the GDPR defines 'recipient' as 'a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not'.
6. Center for Outcomes Research & Evaluation, Yale School of Medicine (2013) 'YODA Project', 19th September, available at: http://medicine.yale.edu/core/projects/yodap/index.aspx (accessed 19th September, 2013).
7. CEO Life Sciences Consortium, 'Share, Integrate & Analyze Cancer Research Data | Project Data Sphere', available at: https://projectdatasphere.org/projectdatasphere/html/home (accessed 7th November, 2019).
8. Transcelerate, 'DataCelerate', available at: https://transceleratebiopharmainc.com/datacelerate/ (accessed 2nd October, 2019).
9. European Medicines Agency, 'European Medicines Agency policy on publication of data for medicinal products for human use: Policy 0070', available at: http://www.ema.europa.eu/docs/en_GB/document_library/Other/2014/10/WC500174796.pdf (accessed 7th November, 2019).
10. Health Canada (2017) 'Public release of clinical information in drug submissions and medical device applications', available at: https://www.canada.ca/en/health-canada/programs/public-release-clinical-information-drug-submissions-medical-device-applications.html (accessed 7th November, 2019).
11. El Emam, K. and Abdallah, K. (2015) 'De-identifying clinical trials data', *Applied Clinical Trials*, available at: http://www.appliedclinicaltrialsonline.com/de-identifying-clinical-trials-data (accessed 12th December, 2019).
12. *Ibid*.
13. 'The YODA Project' (Yale University), available at: https://yoda.yale.edu (accessed 5th February, 2020).
14. Ross, J. S., et al. (2018) 'Overview and experience of the YODA project with clinical trial data sharing after 5 years', *Scientific Data*, Vol. 5, p. 1.
15. The YODA Project, 'Data use agreement', available at: https://yoda.yale.edu/data-use-agreement (accessed 8th February, 2020).
16. See Ross et al., ref. 14 above.
17. See Ross et al., ref. 14 above.
18. There is an exceptions process to gain approval for downloading data in very exceptional cases, for example, where there are technical requirements for the analysis to be carried out that cannot be met within the portal environment.
19. See Transcelerate, ref. 8 above.
20. Yin, P. T., Desmond, J. and Day, J. (2019) 'Sharing historical trial data to accelerate clinical development', *Clinical Pharmacology & Therapeutics*, Vol. 106, p. 1177.
21. *ibid*.
22. See CEO Life Sciences Consortium, ref. 7 above.
23. Green, A. K., et al., (2015) 'The project data sphere initiative: accelerating cancer research by sharing data', *The Oncologist*, Vol. 20, No. 5, p. 464-e20.
24. As mentioned in ref. 18, there is an exceptions process to gain approval for downloading data in very exceptional cases, for example, where there are technical requirements for the analysis to be carried out that cannot be met within the portal environment.
25. See Ross et al., ref. 14 above.
26. European Medicines Agency, 'European Medicines Agency policy on access to documents: Policy/0043', available at: https://www.ema.europa.eu/en/documents/other/policy/0043-european-medicines-agency-policy-access-documents_en.pdf (accessed 17th March, 2020).
27. Hintze, M. and El Emam, K. (2018) 'Comparing the benefits of pseudonymisation and anonymisation under the GDPR', *Journal of Data Protection & Privacy*, Vol. 2, p. 145.
28. *ibid*.
29. See, for example, 45 CFR Parts 160, 162, and 164; Health Information Portability and Accountability Act, Privacy Rule.
30. Drechsler, J. (2011) 'Synthetic Datasets for Statistical Disclosure Control: Theory and Implementation', Springer-Verlag, available at: http://www.springer.com/us/book/9781461403258 (accessed 5th April, 2019); Maynard-Atem, L. (2019) 'The data series — Solving the data privacy problem using synthetic data', *Impact*, p. 11.
31. See Maynard-Atem, ref. 30 above.
32. REGULATION (EU) NO 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF APRIL 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016.
33. 45 CFR Parts 160, 162, and 164; Health Information Portability and Accountability Act, Privacy Rule.
34. REGULATION (EU) NO 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF APRIL 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
35. See Hintze and El Emam, ref. 27 above.
36. Borking, J. J. (2011) 'Why adopting privacy enhancing technologies (PETs) takes so much time', in S. Gutwirth, Y. Poullet, P. De Hert, R. Leenes (eds.), Computers, Privacy and Data Protection: An Element of Choice, Springer, Dordrecht, pp. 309–341, available at: https://www.springer.com/gp/book/9789400706408 (accessed 10th February, 2020); Borking, J. J. (2008) 'Towards Privacy Enhancing Security Technologies — The Next Steps', PRISE Conference Proceedings, available at: http://www.tekno.dk/pdf/projekter/prise/PRISE_D7.3_Concluding_Conference_

Proceedings.pdf#page=43 (accessed 10th February, 2020).
37. Rogers, E. M. (1983) 'Diffusion of Innovations', 3rd ed., Free Press, New York and Collier Macmillan, London; See Borking, ref. 36 above.
38. Office of the Privacy Commissioner of Canada (2017) 'Privacy enhancing technologies — A review of tools and techniques', 15th November, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/ (accessed 10th February, 2020).
39. *Ibid*.
40. See Borking, ref. 36 above; See also Rogers, ref. 37 above.
41. See Borking, ref. 36 above.
42. Kochhar, S., Knoppers, B., Gamble, C., Chant, A., Koplan, J. and Humphreys, G. S. (2019) 'Clinical trial data sharing: Here's the challenge', *BMJ Open*, Vol. 9, p. e032334.