Chapter 10
Defining Data Donation After Death: Metadata, Families, Directives, Guardians and the Route to Big Consent

David M. Shaw

Abstract This chapter explores what we actually mean by data donation after death, and what different types of data donation metadata are involved in the process. It then provides an analysis of the ethical ramifications of each of these different types of data, outlines the concepts of data advance directives and data donation guardians as one way of dealing with these issues, and considers alternative governance mechanisms. The degree of control given to the first data donors may need to be high in order to maintain trust, but over time attitudes may evolve towards everyone giving "big consent" to data donation.

Keywords Data donation after death · Ethics · Big consent · Posthumous data donation · Advance directives · Data guardians

10.1 Introduction

With the advent of the General Data Protection Regulation (GDPR) (EU 2016) and the Cambridge Analytica scandal (Schenble et al. 2018), public awareness of the issues surrounding data governance has never been higher. The GDPR aims to better protect citizens' data rights, while also enabling research and other important activities to proceed under certain conditions. In this context, the very idea of data donation might seem naïve; who would want to donate sensitive data, when 'donation' implies an unconditional gift for the recipient to dispose of as he or she pleases? Data donation after death might be seen as more attractive because the donor can no longer be directly affected by (mis-)use of data, but dead people also cannot raise concerns about any such misuse. In this chapter, I explore what is actually meant by

D. M. Shaw (✉)
Institute for Biomedical Ethics, University of Basel, Basel, Switzerland

Care and Public Health Research Institute, Maastricht University, Maastricht, The Netherlands
e-mail: david.shaw@unibas.ch

J. Krutzinna, L. Floridi (eds.), *The Ethics of Medical Data Donation*, Philosophical Studies Series 137, https://doi.org/10.1007/978-3-030-04363-6_10

"data donation after death" (DDD), and analyse the advantages and disadvantages of various potential governance mechanisms.

I begin by setting out what is meant by DDD in general terms, before illustrating the issues by means of comparison with the established practice of posthumous organ donation. I then explain and analyse the ethical ramifications of the five main types of data donation metadata: whether the related item of medical data can be shared at all, who else is affected by the data, with whom the data can be shared, in what form the data can be shared, and who has authority to change any of the previous four 'settings'. I then sketch the outlines of a potential system whereby donors could impose certain conditions on their data donations. I conclude by considering alternative forms of governance, including ethical oversight of unconditional DDD.

10.2 Defining Data Donation After Death

When people die they leave lots of data behind. This includes financial data, data on social media, governmental and tax data, and personally owned data including (for example) electronic movies and songs, and in some cases creative data such as songs and literary compositions. But for the purposes of this paper, I focus on clinical data and medical research data. When a patient dies he leaves behind not only a medical record, but also any data used in research projects. Despite the person's departure, this data remains an immensely powerful resource, particularly if it can be combined with other datasets. (Indeed, in many cases the nature of the person's departure will also be a relevant data point, if disease linked.) But how can this data be donated? The simplest way to explain DDD is to use organ donation as an example. There are many parallels but also some dissimilarities between DDD and deceased donation of organs (DDO) (Shaw et al. 2015). Both the similarities and the differences are helpful in terms of determining how we should think about DDD and how it should be governed.

In DDO, organs are donated after one's death and distributed among one or more recipients. Consent can come from the donor, via the organ donor register, or from a family member, where there is no record of consent. In 'opt-out' jurisdictions consent can also be 'deemed' or presumed if there is no record of objection. It is important to note that, despite having no legal right to do so, family members often overrule donation even when there is evidence of consent (NHSBT 2017) – this may also be relevant to data donation. DDO is essentially unconditional; no terms can be imposed on who or what type of person can receive the organs (to avoid any discriminatory criteria being imposed), and there are no guarantees that any organs will be transplanted at all. However, donors can stipulate which organs they want to donate; most donors donate all organs, but some choose not to donate specific organs such as the eyes, or the heart.

Should DDD be approached in the same way as DDO? In both cases the patient is dead, and if the language of donation is being used then presumably consent must be given – or at least presumed. Should data donors be able to stipulate who they

donate to, or what types of data? To answer these questions and others we first need to consider the various types of data donation metadata.

10.3 Data Donation Metadata

For each item of data in a person's medical record, or associated research data, there could be several items of metadata indicating that donor's preferences regarding how their data should be used, and setting the terms of their donation. Specifically, each piece of data could(at least) five key data concerning it: whether it can be shared at all; who (if anyone) else it concerns; who it can be shared with; what form it can be shared in; and who (if anyone) needs to give consent for any other type of sharing (see Box 10.1). Each of these must be examined in turn.

First, a person might not want some categories of data to be shared at all. This is most likely to be the case for sensitive sexual health data, or genetic data, which could yield paternity information relevant to other family members. If a category of data is excluded from sharing with anyone, there need be no data regarding it in the second, third or fourth categories of metadata, though there should also be a corresponding entry for the fifth type, as a representative might be empowered to give future consent for this type of data to be shared.

Box 10.1: Data Donation Metadata
Whether it can be shared
Who (if anyone) else it concerns
Who it can be shared with
What form it can be shared in
Who needs to give consent for any other type of sharing

Second, medical data can concern not only the patient to whom it pertains directly, but also his or her family. Though it can also concern other types of medical data, this is particularly true of genetic data. A well-meaning data donor might not consider the fact that if he makes an unconditional donation, it could reveal that his son or daughter also has (or is likely to have) a particular genetic condition, with potential ramifications for privacy and insurance. Should people be able to donate their genetic data when they die? It is "theirs" but it also concerns others, even if this is only in terms of probabilities rather than certainties in many cases, due to genetic data often yielding no definitive answer. In organ donation, families often refuse to give consent to donation or overrule consent because they are upset by the idea of losing 'more' of their relative. Should families have a right to veto data donation, at least in terms of genetic data? In organ donation there is normally little ethical basis for a genuine overrule of what the patient wanted (UKDEC 2016), but given that genetic information can apply to other family members, there are potentially more

solid grounds for legitimate objection. Another possibility would be for the rights of families to be protected by some oversight mechanism such as an ethics committee, but this might be impractical (see next section). (As noted above, non-genetic health information can also yield information on family members; for instance, if a deceased patient had a history of heart disease, this information might be of use to insurers. However, genetic information can reveal definitively whether offspring have or do not have a particular condition, and thus might be regarded as more sensitive.)

Third, people might be happy to donate their medical data posthumously, but not without imposing conditions on who can access that data. For example, evidence from a large UK study suggests that (living) citizens are generally happy to share their data with the National Health Service and associated researchers, rather less happy to share data with university researchers, and downright unhappy to share data with private companies such as the large pharmaceutical ones (Wellcome 2013). People might be more relaxed about sharing data posthumously, but they might also want to exert some degree of control over the potential recipients of their data. If people are denied this control, they might simply refuse to donate any data at all; this was one of the unfortunate features of the ill-fated care.data initiative in England, where patients only had a binary option: either all their data was shared, or none of it at all (Shaw 2014). However, one problem with limiting the recipients of data in this way is that industry often collaborates with the National Health Service (NHS), and vice versa. Ultimately, it transpired that even this simple binary option was too complex; those who opted out had their data shared anyway, indicating the lack of seriousness accorded to data consent in the NHS (Ramesh 2015).

Fourth, data can be shared in four main forms: fully identifiable, de-identified, pseudonymised and fully anonymised. Fully identifiable data reveals a donor's name, date of birth, address, demographics and full medical history. Anonymised data reveals only the medical history, with no location or other data revealed. De-identified data removes personal and demographic information. Pseudonymised information is anonymized data that can be re-linked to patient identifiers using an encoded key (Ohmann et al. 2017). People might be reluctant to share the first of these, but be more content with sharing of pseudonymised data. Generally, people are more comfortable sharing anonymised data as it cannot be linked back to them (Wellcome 2013), but they might be more comfortable sharing de-identified or fully identifiable data in the case of DDD because there is (even) less risk of any adverse consequences to donors who are dead; however, the potential risk to surviving family members remains. It is important to note that in the era of big data and machine learning, de-identified and even anonymised data could potentially be linked with other datasets and thus to specific donors, so the distinctions between these four forms of data are being eroded (Schneble et al. 2018).

Fifth, donors might want to grant authority to a trusted person or organisation to give consent to other future uses of the donated data. This might be prudent because once a person is dead, she can obviously no longer be involved in any such decisions, and circumstances might mean that she would have wanted to change something

were she not dead. By donating, donors give consent to any uses of his or her data within the terms set in their metadata (perhaps subject to further safeguards – see next section). The nominated person would not be required to give consent to all uses of data, but would be approached where a project outwith the scope of the donor's metadata settings wanted to use data.

Finally, it is also important to bear in mind that all of these metadata are interlinked. For example, a person might be happy to share anonymised general medical data with everyone, but restrict use of identifiable medical data and any genetic data to the NHS. They might also be willing to grant authority for a trusted person or organisation to change their preferences for some types of data, but not for all.

10.4 Data Advance Directives

What is the best way to record one's data donation preference metadata? I have previously suggested a data donor card similar to an organ donor card (Shaw et al. 2015) but an instrument for setting preferences in advance already exists in medicine: the advance directive. A data advance directive (DAD) would record all the relevant information mentioned in the previous section, setting the defaults for use of that donor's data.

Setting up a DAD would be a one-time procedure, thought it could of course be altered at any point up to a person's death. Users would be guided through setting up each metadata preference via a decision tree for ease of use. From the initial question - something like "would you like to share your data after death to help researchers?" - questions would probably best be focused on categories of medical and research data, with each group of data having its own metadata preferences as set out above. The second category, regarding who else data concerns, would not be available as a preference but would be set by system guardians. Depending on the jurisdiction, it is possible that genetic data could be shared only with the permission of family members. Thus for each type of data, the user could determine whether to share it at all, and if so (and dependent on whether it also concerns family members) who it can be shared with, in what form, and whether the terms they set for the use of their data can be altered in future by a designated person.

10.5 Posthumous Data Guardians

As stated above, DADs will go a long way towards governing deceased persons' data responsibly. But the final part of setting up a DAD should be to nominate a survivor who can be consulted above any exceptions to the set terms, or potentially to change them permanently. These Posthumous Data Guardians (PDGs) would perform an important backup role, made all the more significant by ongoing rapid

advances in data handling techniques. For example, it might be that in 10 years the category of "de-identified" data will disappear entirely, necessitating a change in DAD preferences to reflect what that user would probably have wanted to do in such circumstances. In addition, some people might not want to set up a DAD, preferring to delegate responsibility for posthumous use of their data to a surrogate. This could be implemented as an option, but would require this person to be contacted for each potential data useage, which would really mean that the data was not donated at all.

10.6 Objections

The combination of DADs and PDGs offers a flexible way for donors to set their preferences and safeguard their (and their families') interests after they die. The main objection to the metadata, DAD and PDG proposal detailed above is that donation should be unconditional, for two main reasons: enabling preference-setting would be against the spirit of donation, and that it would be much more practical to simply have donation of all data.

Is enabling some preferences to be set against the spirit of donation? As already mentioned, organ donors can choose which organs to donate. When people die they can allocate their financial reserves and possessions to wherever they want. Data is highly personal, and if people want to set limits on its use after they are dead, there must be a strong argument against letting them do so – not least because removing the ability to set preferences will push people towards refusing entirely to donate their data.

The second argument about practicality has more force. The more preferences that can be set, the more complicated it is for researchers to combine datasets and some patients' data might be rendered entirely inaccessible. But as stated above, it might be even less practical to alienate donors by not enabling preference-setting.

One other possibility in addition to DADs and PDGs would be to enable donors to set a "data death date" beyond which their data can no longer be used – for example, at 50 years after death. This would set a final boundary on the use of donated data, but it is not obvious that many would find this option attractive. Why share data after your death, but only for a limited period? One potential reason would be that the the risk of unanticipated types of research using ones' data might increase over time, and a time-limit on its use would decrease this risk. However, after decades have passed, a donor's data could have been aggregated and imbedded in thousands of different analyses, and stopping use of it might be highly impractical even if there was a good reason for allowing donors to set such an expiry date. Allowing control so far beyond the grave would also constrain the public benefits flowing from the initial donation.

10.7 Other Governance Mechanisms

Taken together, even for just one person, the amount of data involved in DDD means that we are essentially talking about big data, and hence not simply data donation but actually 'big data donation'. That in turn means that what is needed is big data protection; protection not only of the data concerning an individual, but also of the potential benefit to the public of big data research (Shaw 2017). DAD would be one way of providing this. But if we were to reject detailed preference-setting as set out above, and aim to embrace a less controlling, more openly altruistic model of data donation, what alternative governance mechanisms exist?

One option would be for donation to be regarded as broad consent to future research, subject to future research ethics committee (REC) review. This option already exists outwith the context of donation; in many consent forms, participants can not only agree to take part in a given study, but also for their data or samples to be used in any future study, subject to REC review. This model could work, but suffers from two main drawbacks. First, giving certain limited data and perhaps one or two biological samples is rather different from donating all the medical data ever generated about yourself. Donating unconditionally all your medical and genetic information and trusting RECs to always approve only 'safe' projects may be asking too much of potential donors, particularly in the coming era of ethics review equivalency, where some have suggested that additional REC review may not be required when new countries start participating in a study. Second, any unconditional donation will last essentially forever. Setting preferences and nominating a guardian at least offers some degree of control over future use of data.

Another alternative would be a move towards not research ethics committees, but research ethics communities, where it is assumed that everyone will contribute their data both while living and once dead in order to show solidarity with and benefit their community (Shaw 2017). This would be the ideal solution; a world in which everyone unconditionally donates their data. But it may be unrealistic to try to step straight to such a world. The combination of DADs and PDGs in DDD is a safe first step towards encouraging people to trust researchers with their data. Following this, the use of this preference scheme could be extended to data donation whilst alive, before trialling unconditional donation after death and ultimately a community where everyone shares their health data all the time. Notably, any such research ethics community would at a stroke solve the issue of family data sharing – if all family members share data routinely through solidarity, no concerns about genetic information need remain.

However, families remain an issue for unconditional data donation in the present day. While many, or even most relatives might be happy for their family members to donate genetic and other data when they die, others might not, and it is difficult to see how someone can donate data that is not entirely theirs, as it is thus not entirely in their gift. The fact that genetic data concerns not only ourselves but also our family members may be a significant barrier to the very concept of data donation.

It might be objected that family members have no say in whether we share our genetic or other medical data while we are alive; why, then, should they have a say when we are dead? It is true that each living person is free to share any personal medical information that he or she pleases with researchers, without constraint by any relatives. However, this is because a living person has certain rights regarding his or her data, even if it affects their family members. Once that person is dead, the only people that can be directly affected by use of that data are the deceased's family members, and the balance of control should shift accordingly – not entirely to the family, but towards shared control over the data.

For this reason it might be better to think in terms of dual consent to data donation after death, rather than simple data donation after death. A person can consent to donation, and this donation can proceed only if potentially affected family members also consent. A data donor can consent to use of his or her data, but cannot consent regarding data that also concerns family members. Therefore, a type of dual consent might be required for full data donation after death. This is unfortunate, but the path towards full data sharing will not be paved with good intentions if families are not on board with the first models of data donation. Ultimately, as stated above, a move towards a research ethics community, where every one is happy to give not specific or narrow, nor broad, nor general but 'big consent' to all use of all 'their' big data without restrictions, whether or not it concerns their family members.

10.8 Conclusion

In this paper, I have suggested that, while DDD could ultimately be unconditional, any such scheme must begin by allowing donors to set certain preferences. Encouraging potential donors to create data advance directives is the first step towards a world in which data sharing for the common good is 'automatic for the people', both in the sense of being a common good, but also being second nature. The route to big consent must begin with dual consent to data donation.

References

General Data Protection Regulation (GDPR) (EU) 2016/679.

National Health Service Blood and Transplant. 2017. *National potential donor audit*.

Ohmann, C., R. Banzi, S. Canham, et al. 2017. Sharing and reuse of individual participant data from clinical trials: Principles and recommendations. *BMJ Open* 7: e018647. https://doi.org/10.1136/bmjopen-2017-018647.

Ramesh, R. 2015. NHS disregards patient requests to opt out of sharing medical records. *The Guardian*, 22nd January 2015. https://www.theguardian.com/society/2015/jan/22/nhs-disregards-patients-requests-sharing-medical-records. Accessed 21 Aug 2018.

Schneble, C.O., Elger, B.S., and Shaw, D. 2018. *The Cambridge Analytica affair and Internet-mediated research*, EMBO reports 2018. Online early. https://doi.org/10.15252/embr.201846579.

Shaw, D. 2014. Care. data, consent and confidentiality. *Lancet* 383: 1205.

———. 2017. Ethics review equivalency, moral jurisdiction and research ethics communities. *Medicine and Law* 36: 51–59 big data protection.

Shaw, D., J. Gross, and T. Erren. 2015. Data donation after death. *EMBO Reports* 17: 14–17. https://doi.org/10.15252/embr.201541802.

UK Donation Ethics Committee (UKDEC). 2016. *Involving the family in deceased organ donation: A discussion paper*. Academy of Medical Royal Colleges.

Wellcome Trust. 2013. Summary report of qualitative research into public attitudes to personal data and linking personal data, July. Available at: http://www.wellcome.ac.uk/About-us/Publications/Reports/Publicengagement/WTP053206.htm.