Privacy and Responsible Information Sharing

I am a member of the general public wishing to comment on this poor excuse for privacy legislation which affects the rights of all of us for the benefit of a small few. I have read through all 52 pages of the Discussion Paper and found it to be nothing other than a plea from entitled bureaucrats and researchers to be able to access our data without restriction and to do away with decades of privacy protections which have been built up to protect that data, and through them, our dignity. This proposed privacy framework does little to protect our data, and instead exposes it to cyber security breaches by allowing greater online sharing, and strips us of our consent rights for how our data can be handled.

Of particular concern to me is that this framework essentially forces ehealth on us as patients and removes all rights we have to say no to that. I have opted out of the My Health Record, yet this privacy framework would allow my health information to be shared online regardless, in direct conflict with my instructions not to. I was young and naive when I first saw a doctor. I had a naive belief that it would be confidential and that she couldn't share my medical records without my consent unless there was a threat to the safety of myself or others. Whatever trust I had back then has all but dissipated through the slippery slope into involuntary ehealth that has occurred in the years since. I have never given my consent to ehealth, yet it has gradually been forced on me anyway by default, leaving me having to jump through multiple hoops to try to prevent it. And my trust with doctors has disintegrated as a result. It has.

This framework does not do the one main thing the general public would expect it to, which is to give us greater control to prevent the sharing of our data. Instead, it does the opposite, allowing organisations to share our data more widely without needing to seek our consent first, and without any obligation to respect our wishes if we ask them not to. Nor are there any "tell us once" settings to protect our privacy and prevent data sharing, only to allow it. Where is the setting to say no to all ehealth, or all online sharing of data?

1) What issues should be considered when developing privacy and information sharing legislation for Western Australia?

- It should consider the potential detrimental effect on patient trust when consulting doctors
- It should consider personal security risks that arise from sharing contact details
- It should consider our individual liberties to make decisions for ourselves as free citizens in a liberal democracy
- It should consider that we are the true owners of our data and should respect our rights

to control the sharing of that data

- It should at a minimum give us the option to prevent online sharing of data given the significant risks of cyber security breaches
- It should consider that the general public do not have blind faith in dubious claims of data security
- It should consider the significant risk of re-identification of data and the lack of public trust in the de-identification process

2) What privacy principles should WA adopt for regulating the handling of personal information by the public sector? Are any of the existing Australian Privacy Principles, or principles in other Australian jurisdictions, unsuitable for WA?

- The APPs are quite weak, allowing for cross-border data sharing, direct marketing, and restricting us to access and correction of our data instead of to deletion of it or to prevention of it being shared
- Privacy principles should recognise that "access and correction" does not respect our ownership of our data and should instead allow us to prevent data from being shared outside of a threat to the safety of self or others
- Cross-border data sharing should not be allowed except with specific consent
- Direct marketing should not be allowed except with specific consent
- Government identifiers should not be allowed to be used for data linking except with specific consent, as this affects patient trust
- Data accuracy principles should not overrule our right to control what we choose to share with doctors, dentists or other allied health professionals
- Unsolicited personal information principles should not overrule our right to choose what we share with doctors, dentists or other allied health professionals
- Anonymity and pseudonymity should not be restricted in the health sector as this is vital for patient trust, especially given the erosion of our rights to say no to ehealth
- Privacy consent forms should offer itemised consent options

3) What should the role of a Privacy Commissioner be, and how can this role best protect privacy and ensure public trust?

- The role of a Privacy Commissioner should primarily be to protect our privacy, not to allow it to be trampled on, as this framework seeks to do
- They should be able to fine organisations or individuals who do not adequately protect privacy or respect our consent rights, and they should be able to refer cases for criminal prosecution where relevant

- The role of a Privacy Commissioner should not be at the expense of existing criminal penalties for mishandling of data

4) How should breaches of privacy be managed, and what action should be taken in response to a breach?

- There should be an option for criminal penalties including prison sentences, not just fines
- This could include the Privacy Commissioner referring breaches to police, and should protect the identity of individuals who have had their privacy breached
- There should be mandatory notification of privacy breaches, in line with federal laws

5) When should government agencies be allowed to share personal information? Are there any circumstance in which it would not be appropriate to do so?

- Only in a way that respects our consent rights, except where there is a threat to the safety of self or others
- Health information especially should not be shared without consent as this destroys patient trust
- At a minimum, we should be able to prevent our data from being shared online given the significant risks of cyber security breaches
- It would not be appropriate where there is a personal security risk from sharing contact details, such as in witness protection or family violence cases
- It would not be appropriate for whistle-blowers

6) What should the role of a Chief Data Officer be? How can this role best support the aims of Government and the interests of the public?

- This role should not exist as it is an attack on our privacy rights
- Data sharing and linkage should not occur without our consent
- This privacy framework is a poor excuse for privacy legislation, which does more to strip us of our privacy than to protect it

7) Should the WA Government facilitate sharing of information outside the WA public sector? What should be considered when making a decision to share outside the WA public sector?

- No, it also shouldn't facilitate sharing of information within the WA public sector either
- The proposed framework strips us of our consent rights to control how our data is handled and does little to protect our privacy
- What should be considered is the detrimental effect that data sharing and forcing ehealth has on patient trust

- What should be considered is that we are the true owners of our data and that as free citizens in a liberal democracy we should be the ones to decide how it gets shared

8) What criteria should be included as part of a risk management framework such as the Five Safes?

- The Five Safes framework does not adequately represent the risks of data sharing
- "Safe data" does not pay enough consideration to the significant risk of re-identification of data, nor does it reflect the lack of trust the general public has in the de-identification process
- De-identification processes frequently allow birth dates to be retained, which can be combined with suburb or gender to re-identify data
- "Safe people" does not respect our right to choose who we trust
- "Safe setting" does not respect our right to control how our data is handled, and does not adequately represent the risks of sharing data online, or the effect on patient trust
- "Safe setting" also does not consider the lack of trust the general public has in dubious claims of data security
- "Safe outputs" does not adequately consider the significant risk of re-identification of data, or the effect on patient trust
- "Safe projects" does not respect our right to control how our data is handled, or the effect on patient trust from data sharing

9) Under what circumstances would it be considered acceptable to share confidential information within the public sector?

- This should not happen without consent unless there is a risk to the life or self or others
- Health information especially should not be shared without consent as this destroys patient trust
- At a minimum, we should be able to prevent our data from being shared online given the significant risks of cyber security breaches

10) What should the WA Government be doing to support successful implementation of privacy and information sharing?

- "Privacy" and "information sharing" are opposite concepts
- Privacy is about limiting the sharing of data and allowing us to control how our data is handled, shared, and stored
- Information sharing is about reducing limitations on sharing data and stripping us of our consent rights to control how our data is handled

- The information sharing proposed in this framework tramples on our privacy rights and our individual liberties
- This framework is a poor excuse for privacy legislation which strips us of our rights to control how our data is handled and should be scrapped
- Health information especially should not be shared without consent as this destroys patient trust
- At a minimum, we should be able to prevent our data from being shared online given the significant risks of cyber security breaches

This proposed framework does not protect our privacy. This framework strips away decades of privacy protections which were built up to protect our data, and through them, our dignity as human beings. This framework would expose our data to significant risks of cyber security breaches, re-identification of data, and misuse by any of the thousands of people it would be shared with. This framework also dessimates patient trust by essentially forcing ehealth on us, and removing any rights we have to say no to that. I have opted out of the My Health Record, but this framework would ignore that and force online sharing of my health information on me anyway, in direct conflict with my instructions not to. Involuntary ehealth has dessimated my trust in doctors and this will only worsen that, for me, and for others. Please protect our right to keep our health information offline.