Health Legislation Amendment (eHealth) Bill 2015

1. Introduction

I am a patient with no experience working in the health or IT sectors, writing purely from the perspective of a patient. I am writing to voice my opposition to ehealth changing from opt-in to opt-out and especially to third party information being allowed to be included, as this denies patients the opportunity to truly opt out.

I have included with this submission the submission I made to the *Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper* earlier this year.

2. Contents

1. Introduction
2. Contents
3. Third party information
4. Security risks and potential consequences
5. Human rights assessments
   5.1 Right to health
   5.2 Protection of privacy and reputation
   5.3 Right to an effective remedy
   5.4 Rights of people with a disability
   5.5 Protection of children and families
6. Removal of protections
7. Copyright & ownership
8. Excessive data retention periods
9. One-sided consultation process
10. Scope creep
11. Remaining questions
   11.1 Does "effective removal" of documents completely remove them, or just hide them?
   11.2 Will any types of information be excluded by default?
   11.3 Can patients block healthcare providers from writing to the system, or only reading?
   11.4 Are there protections against opted-out patients being opted back in by next of kin?
   11.5 Are records of requests made to the HI Service or the My Health Record stored for patients who have opted out and can patients delete entries from logs?
   11.6 Are "classes of healthcare recipients" based only on location, or also on health information?
   11.7 Can patients choose preferred method of contact?
12. Alternatives to an opt-out model
13. Summary
14. Appendix

3. Third party information

This bill seeks to allow third party information to be included in patients' online records, contrary to the wishes of those third parties who may have chosen to opt out. Speaking as a patient who doesn't want any form of ehealth, I would see this as completely defeating the purpose of allowing me to opt out, if my health information were to be uploaded anyway into my family's records. I have zero trust in the security of online storage systems, and I especially don't want my medical information in them. For me, having that information stored in family members' records - where I would be identifiable by my relationship to those family members - would be no different to having it stored in my own record.

That point about identifiability is important. While the third party may not be named in the patient records, their relationship to the patient would significantly narrow down who it could be referring

to. People generally only have one mother or father and only a handful of sisters, brothers or grandparents. So if this system were ever subject to a large-scale hacking and the health information it contains were made public, then people who know the patient and their family would easily be able to guess the likely identities of the third parties. Third party information should, therefore, only be allowed to be included with the express consent of those third parties, if at all.

This may also have relevance to abusive family situations. For most people, they may be able to avoid having their health information included as third party entries into other people's records, simply by asking their family members not to allow it. However, that might not be possible in less healthy family situations, where that request could be met with the opposite outcome by an emotionally abusive family member. This outcome could include not just the uploading of true information that the third party doesn't want shared, but also of untrue information.

The power to decide what health information is uploaded about a patient should lie with that patient, not with their families or with the doctors of their family members. Allowing third party information to be included would make a mockery of the claim that patients can opt out, or that they are in control of what gets shared.

Some of the clauses that allow third party information can be found at:

Items 74 and 75 (page 54)
Item 84: Section 58 (page 60)
Item 106: Schedule 1, Part 2, Division 2, Clause 7 (page 82)
Item 106: Schedule 1, Part 2, Division 3, Subdivision A, Clauses 9(2) and 9(3) (page 89)
Item 110 (page 94)
Item 125 (page 98)

Clause 7 and Section 58 mentioned above are broad powers which don't limit whose records the health information can be inserted into.

4. Security risks and potential consequences

This bill is being introduced in the wake of a series of high-profile hacking incidents, such as the Ashley Madison hack, the mass leak of celebrity photos and videos online and the hacking of various government departments internationally. Any online storage system is vulnerable to outside attack and this system is no different. In this case, given the sensitivity of the data involved, any hacking incident that does occur could lead to severe embarrassment or humiliation for the patients whose data is hacked and ongoing psychological distress. Ehealth is often compared to online banking, but that comparison ignores the different sensitivity levels of the data involved. Dignity can't be refunded in the same way money can.

If and when a significant hacking event does occur, this may lead to a loss of trust in doctors for the patients involved, which may in turn lead them to withhold information on later visits, or to avoid seeking treatment altogether. Even just a fear of that hacking event, or a sense of being stripped of control could lead patients to be less open in sharing information. For me, I'm already wishing I hadn't told my doctor certain things in the past, and am also regretting sharing health information with my family given the third party permissions included in this bill. It's worth remembering that one of the principle tenets of medicine is to first do no harm. This can do harm.

5. Human rights assessments

The explanatory memorandum (EM) for this bill argues that it is compatible with international human rights standards with regard to the following rights.

5.1 Right to health

The assessment provided in the EM fails to consider the risks of loss of patient trust and the effect that would have on how comfortable a patient feels seeking treatment and speaking freely with their healthcare professionals. If patients fear having their medical records uploaded online, either now or in the future as a result of further legislative changes, then that can lead to them withholding information from their doctors or avoiding seeking treatment altogether. This effect would be magnified in the event that the security of this system is ever breached, especially if the patients weren't aware they even had ehealth records. The right to health includes not just having access to health services, but also feeling able to access them.

5.2 Protection of privacy and reputation

When there is a high likelihood of a security breach, this can't be considered to be respectful of privacy. Many patients won't know they even had a record until after it is breached, such as those with language or disability barriers, and hence won't be able to either opt out or adjust the privacy settings. Any claim that this is compatible with the right to protection of privacy is questionable.

5.3 Right to an effective remedy

I would note here that there is no mechanism provided to prevent your health information being uploaded as third party information into family members' records, or to remedy this if it happens.

5.4 Rights of people with a disability

The greater emphasis on the wishes of the disabled being taken into account is welcome and is one of the few parts of this bill that should be passed. That said, that doesn't make up for the risk that many disabled people will have this forced on them without them knowing, or without them fully understanding the privacy implications. Whether they are asked their opinion may depend on the knowledge of a carer, and the opinion they give could be heavily influenced by how it is presented to them. For disabled people who are unable to give an opinion, there are no safeguards included to protect them from having especially sensitive health information uploaded where any potential benefit may be outweighed by the risks associated with a data breach.

It is also possible there may be an impact with the ID requirements for opting out, though it does seem an attempt is being made to make this process as easy as possible. I would suggest amending the legislation to prevent those ID requirements from being tightened in the future.

5.5 Protection of children and families

My comments on the rights of people with a disability apply here to children as well. Additionally, protection of families could include protection of individual family members against having their wishes over-ruled by other family members through the permissions for third party information to be included in records. As noted earlier, this could potentially include cases where the powers are used as a tool of emotional abuse against the third parties.

6. Removal of protections

The bulk of this bill appears to be aimed at removing the protections that were included in the original legislation against excessive collection, use and disclosure of private information. My understanding is these protections were put in place to protect patients against people going on fishing expeditions to find out their health information. With the large number of people working in the healthcare sector, it is likely that any given patient would have friends, family, former partners, old schoolfriends, work colleagues etc who would have access to the portal and who may be tempted to snoop. While penalties after the fact may be of some small comfort to a patient who has had their privacy breached, prevention would be preferable. This bill has a feeling of carelessness in how many protections against disclosure it is removing.

7. Copyright & ownership

As I noted in my submission to the draft legislation discussion paper, I find the idea of doctors being able to claim any sort of ownership rights over patient medical records to be ridiculous. I consider my medical records to be an extension of my body. They are about me, about my body. I should therefore own them just as completely as I own my body. The idea of doctors and health organisations claiming any sort of ownership rights over them, or copyright or intellectual property, is, in my eyes, akin to them claiming ownership or copyright over my body. Ideally, I would like to see all copyright permissions relating to medical information removed from doctors and given to the rightful owners - patients.

8. Excessive data retention periods

This bill still allows for excessively long data retention periods of 30 years after a patient dies, or 130 years from their date of birth if their date of death is unknown. I don't see the justification for keeping our sensitive medical data for such long time periods, and even moreso if the data has been provided without our consent or if we've asked for it to be deleted? A more appropriate time period would be six months after death, and even that is a bit long. Ideally though, it should be the patient's decision.

This is especially relevant where the patient was unaware that their medical records were being uploaded to the My Health Record system. If their medical information has been shared without their consent, they should be able to request that the person or persons it was wrongly shared with not be allowed to keep a copy. Consider also how it looks for a government department to collect patient medical records without their consent and then insist on keeping it for up to 130 years.

The final point is that those lengthy data retention periods open up the possibility of the data being kept for even longer time periods, or perhaps indefinitely if a future government amends the law to allow for that. The longer the data is kept, the greater the risk of it being subject to further time extensions.

9. One-sided consultation process

Much of the patient consultation so far has been conducted with patients who have willingly participated in ehealth and who are coming from a starting position of wanting and supporting it. By only engaging with these patients and not with those who don't want ehealth, this creates a perception bias where patients are seen as being generally supportive of the concept. This, combined with a lack of media coverage of the inquiry processes, may have created a situation where only supporters of ehealth are informed of and involved in consultations, skewing the results in favour. For instance, I only found out about the draft paper earlier this year after a chance visit to a pro-ehealth website days before the submission due date.

As I mentioned in my submission to that discussion paper, the methods used to consult patients tended to be group-based, such as workshops and group teleconferencing. The group nature of those methods may exclude people who are naturally protective of their privacy, people who are shy or who have a fear of public speaking, or people who suffer from more embarrassing medical conditions. This again, could skew the results towards patients who are more open to sharing and away from those who value their privacy more.

The explanatory memorandum also quotes a figure from international ehealth systems showing an opt out rate of approximately 1%. I would question whether this reflects the genuine rate of desire for opt out, or whether this is due to some other factor, the most obvious being lack of awareness of either the records system or of the ability to opt out. A split of 99 to 1 wouldn't ring true for very many issues at all. It also raises the question of how that 1% felt about being forced to opt out? What effect did the whole experience have on them?

10. Scope creep

The explanatory memorandum mentions the possibility of future regulations to authorise new agencies or entities to collect, use and disclose information under limited circumstances. The examples given are the NDIA and cancer registeries. Would these powers allow for any scope creep to include other government bodies such as Centrelink or law enforcement?

11. Remaining questions

11.1 Does "effective removal" of documents completely remove them, or just hide them?

When a patient 'effectively removes' documents from their records, are they completely removed, or are they still in the system, hidden to doctors, but accessible to hackers? This is especially relevant for documents which have been uploaded without consent.

11.2 Will any types of information be excluded by default?

Given the risk of security breaches and the possible effect on patients, are there any safeguards in place to ensure the most sensitive information is not uploaded without consent? As a start I would suggest:

- any images or descriptions of genitals or breasts - to upload this without consent would be akin to so-called 'revenge porn', for want of a better term
- information relating to victims of crime
- any information relating to the fields of urology, obstetrics, gynaecology, sexual and reproductive health or bowel health
- abortion services or counselling
- mental health information and therapy notes in particular
- information relating to sexual orientation or gender identity
- anything which carries the stigma of patient blame, such as weight and smoking related illnesses
- anything at all on patients either known to be sensitive to privacy issues or who are suffering from mental health conditions which could indicate this eg social phobia

11.3 Can patients block healthcare providers from writing to the system, or only reading?

Discussion has focussed on patients wanting to block providers from reading certain documents, but are there full controls to also block providers from *writing* to the record without consent? Writing would bother me more than reading, when I see anything online as essentially in the public domain. Do patients have the option to only allow specific document uploads on a case-by-case basis, with a blanket ban on any document that hasn't been pre-approved? How fine-grained are the patient controls?

11.4 Are there protections against opted-out patients being opted back in by next of kin?

If a patient has opted out, but later becomes incapacitated, is it impossible for next of kin to re-register them against their wishes? The section on disability seeks to ensure that the wishes of disabled patients will be respected if known, but is a prior decision to opt out a guaranteed protection? If a formerly opted-out patient is ever re-registered without their knowledge, will they be informed? This again could have relevance in abusive family situations.

11.5 Are records of requests made to the HI Service or the My Health Record stored for patients who have opted out and can patients delete entries from logs?

I agree with the general logging principles to monitor who has attempted to access a record, but do patients have the ability to delete entries from the log if they reveal too much information about what treatment they are seeking and where? And what logging is kept for patients who have opted out - will there still be a list somewhere of every healthcare provider they have sought treatment from who has attempted to call up their record and HI number, even if those requests were rejected

due to the opted-out status of the patient? If so, then this could, as with third party permissions, defeat the whole purpose of opting out.

11.6 Are "classes of healthcare recipients" based only on location, or also on health information?
The bill gives the Minister power to apply the opt-out trial to "a class, or classes, of healthcare recipients", but doesn't rule out those classes being based on criteria other than location. If health information is included as a factor in determining the classes of recipients, then could this reveal health information about the people who opt out just from their eligibility to opt out? Or would everyone in the trial location be able to opt out, even if they didn't meet the criteria for the prescribed classes of recipients?

The relevant clause for this is at:

Item 106: Schedule 1, Part 1, Clause 1 (page 79)

11.7 Can patients choose preferred method of contact?
The bill allows the System Operator to contact patients by email or SMS if available. Do patients have any option to choose their preferred order of contact or to restrict any methods they aren't comfortable with, for instance, if they know someone else may be likely to read their text messages?

12. Alternatives to an opt-out model
Has the third option of pushing patients to make a decision been considered? Or retaining the opt-in system but sending out invitation letters and forms to complete? Either would be better than an opt-out system which would result in non-consenting patients having their sensitive medical records exposed to hackers and excessive information shared with their dentists.

13. Summary
In summary, the proposal to change to an opt-out system should be rejected due to the humiliation, psychological distress and loss of trust patients may feel if their sensitive health information were ever to be hacked in a 'privacy Chernobyl' type of event. If parliament does proceed with the change to opt out, then third party information should be excluded from the My Health Record, as to include it makes a mockery of the claim that patients can opt out, if their medical history can be uploaded anyway as part of their family members' records.

As a patient, I value my privacy. I don't consider any online storage system to be secure, especially in light of recent high-profile hackings. If opt-out is introduced, then I want to be able to opt out fully and to ensure that none of my health information is recorded anywhere within this system - not in other people's family histories, not in logs of requests made to the HI Service, not through meeting criteria to be a member of a 'class of recipients', not through next of kin revoking my decision to opt out, nor through any other means.

In general, patients should be given more oversight over how their medical information is shared, not less. We need more information on every registry, every repository, every portal, every database, every archive, every index, every cloud, every digitalisation, every record our data has been sent to and to be given a chance to control that process.

14. Appendix
Attached is a copy of my submission to the *Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper.*

H. Nichols

Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper Submission

Background

I am writing this submission as a patient with no experience working in the health or IT sectors, writing purely from the perspective of a patient. I am writing primarily to voice my objection to the change to an opt-out model, which I feel is a betrayal of patient trust and a denial of our right to give informed consent.

Current political and social climate

This debate is happening against the backdrop of a spate of online data breaches, including breaches of data held by US government agencies such as the US Office of Personnel Management. It is also happening against a backdrop of compromising celebrity photos and videos being hacked and distributed online, and of 'revenge porn' attacks, for want of a better term. These breaches would have a cumulative effect on the public's trust in the security of any ehealth system.

Objection to opt-out model

Given the sensitivity of health data and the security risks associated with online databases, I feel that medical information should never be put online except with explicit consent from the patient. This can only be achieved through an opt-in consent model where the patient knows about and is fully consenting to the information sharing. There is no such thing as "opt-out consent". Consent entails knowledge and involvement in the process.

Third party information

One thing that especially alarmed me in the discussion paper (paragraph 170) is the plan to allow third party information to be included in ehealth records. This makes an absolute mockery of the idea of patients being able to opt out of ehealth, if their data can still be included in the records of relatives against their wishes. If a patient feels violated by their medical records being uploaded to the internet, how can you justify ignoring their wishes and allowing their medical information to be uploaded anyway?

As it is not possible for a clinician to know whether third parties have consented to ehealth or not, and as these third parties may be identifiable by their relationship to the patient, the only appropriate solution is to err on the side of caution and not allow third party information to be included in PCEHR records unless consent can be obtained.

Pros vs cons

The discussion paper seems to only acknowledge the benefits of ehealth, without considering the harm it can do to patient trust. If patients feel their privacy has been breached and their trust broken by having their medical records uploaded online, then that can lead to an obvious consequence of them withholding information from their doctors on later visits. The fear of future changes which strip us of our right to choose altogether, and the inevitability of hacking incidents would also have this effect. Ehealth is only of benefit when the patient is in full control over the process and can choose at every stage what information can be included in, or fully withdrawn from, their record.

Ownership

As a patient, I consider my medical records to be an extension of my body. They are about me, about my body. I own them, or should own them, just as completely as I own my body. So the idea of doctors and health bodies claiming any sort of ownership rights over them, or copyright or intellectual property, is, in my eyes, akin to them claiming ownership or copyright over my body. Ownership over medical records should be considered to belong entirely to patients and no one else.

I would also suggest initiating this conversation between doctors and patients, as I suspect many doctors don't realise that patients may be offended by, or at least disagree with, the idea of anyone owning their medical records besides themselves.

Degrees of violation

I'm not sure the authors of the discussion paper understand the level of violation patients may feel if their medical information were to be put online without their consent, or if it were to be hacked. While the privacy violation is obvious, it goes beyond that into also being a bodily violation and in some cases, a sexual one. If the information uploaded without consent relates to fields such as gynaecology, obstetrics, urology or sexual health, and especially if it contains any photographic or xray images of the groin region or breasts, then I'm sure most women would feel violated by that on a far deeper level than with other privacy violations. Whatever the intentions may be for uploading such data to an ehealth record, the feelings that situation would elicit would be in some way comparable to those experienced by the victims of 'revenge porn'. No images or intimate descriptions of people's bodies should ever be uploaded to the internet without consent.

I would make the point that proponents of ehealth seem to be thinking in terms of minimally sensitive information such as allergies, whereas patients immediately think of their most sensitive information, whatever that may be.

Alternatives to opt-out

Has the third option of pushing patients to make a decision been considered? Or retaining the opt-in system but sending out invitation letters and forms to complete? Either would be better than an opt-out system which would result in non-consenting patients having their sensitive medical records exposed to hackers and excessive information shared with their dentists.

Ease of opting out

If you do decide to override patient consent by switching to an opt-out system, the methods available to opt out need to be as easy and accessible as possible. Multiple methods should be available, including in person, by mail, online and by phone. ID requirements also should not be so stringent that patients are unable to exempt themselves. The discussion paper only mentions driver's licences, passports and Immicards, but there would be many people with none of the three, or with no photo ID at all, or who cannot complete a 100 point ID check. Every effort should be made to allow flexibility in ID requirements to enable people to opt out.

The requirement for the secretary to write to the last known address to confirm the opt-out is also problematic for anyone suffering homelessness, escaping a domestic violence situation, or who is hospitalised or incarcerated. While I understand the reason for this, it would make it impossible for many people to complete the opt out process. Some flexibility is needed surrounding this rule also.

The right answer though is not to change to opt-out at all. Too many patients will be unwittingly caught in this who are unable or unaware of how to opt out, for a variety of reasons such as language barriers, ID requirements, incarceration or hospitalisation, homelessness, or diminished decision-making ability, but who would still feel their trust had been betrayed regardless. As a matter of principle, patients should have control over their medical information, including that it should never be uploaded to the internet without explicit consent.

Trial sites

With the trial sites, is it possible anyone could be caught inadvertently because they live outside the trial region, while their doctor's practice is inside; or because their previous address is inside the trial site and they haven't updated their Medicare records yet? Could the opt-out process be available nationally from the start of the trial period to guard against this?

Data retention periods

Both the discussion paper and the existing legislation allow for an extraordinary length of data retention, with a retention period of 30 years after the patient's death, or 130 years if the date of death is unknown. I don't see the justification for keeping our sensitive medical data for such long time periods, and even moreso if the data has been provided without our consent? A more appropriate time period would be 6 months, up to a maximum of 2 years, though preferably the patient should have input into the decision.

This is especially relevant where the patient was unaware that their medical records were being uploaded to the PCEHR. If their medical information has been shared without their consent, they should be able to request that the person or persons it was wrongly shared with not be allowed to keep a copy. Consider also how it looks for a government department to collect patient medical records without their consent and then insist on keeping it for 30 or 130 years.

The final point is that those lengthy data retention periods open up the possibility of the data being kept for even longer time periods, or perhaps indefinitely if a future government amends the law to allow for that. The longer the data is kept, the greater the risk of it being subject to further time extensions.

Patient controls

In line with the concept of patients being in control of their own records, the system should be reviewed to ensure patients do have the controls that they may not have been granted in the original PCEHR system. Patients should have the ability to completely remove documents from their record, rather than just being able to hide them in a locked, but still accessible, envelope. If a document has been uploaded without the patient's consent, or if they changed their mind afterwards, they should be able to completely remove the document, otherwise they would be left with opting out of the PCEHR as their only option to remove the document.

Patients should also have the ability to block emergency access to any documents they choose, and to request that a patient approval mechanism (such as a password) apply to the upload of each and every document. The ability to technologically block uploads should extend to individual documents, not just healthcare providers.

Paragraph 195 of the discussion paper under the heading "Retaining information for security purposes" would allow the PCEHR System Operator to collect and disclose more personal information. This should only be allowed with patient consent.

Clause 3.4.7, Paragraph 151 would give the System Operator flexibility to contact the patient by methods such as email, SMS or phone. This is fine, so long as the patient can choose their preferred order of contact and to request that some forms of contact not be used, such as banning phone contact if they know their phone may be answered by someone else.

Expanding criminal penalties

I would cautiously support the introduction of criminal penalties for breaches of the PCEHR Act, including imprisonment, so long as it is solely the patient's choice whether to pursue it through that avenue, or through the civil avenues currently available. Breaches of health information should be considered a serious matter worthy of imprisonment, however, this is a process that would involve the patient's sensitive health data being presented in a courtroom, in front of a jury of 12 people, a magistrate, lawyers and possibly the media and members of the public. That should only be allowed to occur with the patient's informed consent.

I don't see any need to reduce penalties for breaches of the HI Act.

Obligation to use PCEHR for some Medicare items

Clause 3.4.6, Paragraphs 145 - 147 suggest requiring certain assessments to be uploaded to a PCEHR record if one exists, without paying any regard to the sensitivity of the information contained and not much to the patient's wishes. The list of Medicare items include mental health plans which are highly sensitive in nature; chronic disease plans which would include stigmatised conditions such as those related to obesity and smoking; medication reviews, health assessments and comprehensive assessments which could contain anything. This, and any other proposal to obligate that a specific document type be uploaded, should be rejected in favour of respecting patient consent and control.

PCEHR policy for organisations

I support organisations being obligated to develop a policy to deal with matters relating to the PCEHR, such as staff training, security breaches and information handling (Clause 3.4.3, Paragraph 140). I would like to add one suggestion however, about reducing the subtle social pressure on patients to consent to ehealth by restricting conversations about it in public areas such as waiting rooms, pharmacies and shared hospital rooms. Asking patients too many questions about their decision to opt in or out of ehealth in public areas can exert a subtle pressure on the patient to agree to something they aren't really comfortable with in order to avoid an awkward conversation with an audience. Organisations' PCEHR policies should therefore contain guidelines on minimising discussions about ehealth in the presence of other people unnecessarily.

Consultation process

The consultation process to date is described in the discussion paper as having been focussed mostly on public consultation methods such as workshops and group teleconferencing. While these methods have their place, I would like to point out that the group nature of them may exclude people who are naturally protective of their privacy, people who are shy or who have a fear of public speaking, or people who suffer from more embarrassing medical conditions. This in turn may skew the results in favour of those who are more positive towards ehealth and against those who have concerns about security and privacy.

Likewise, much of the patient consultation so far has been conducted with patients who have willingly participated in ehealth and who are coming from a starting position of wanting and supporting it. By only engaging with these patients and not with those who don't want ehealth, this creates a perception bias where patients are seen as being generally supportive of the concept. Perhaps sending out anonymous questionnaires to randomly selected participants might bring in a broader cross-section of the public?

PCEHR vs My Health Record

While it's not a big issue, I'm not really in favour of the name change. I like the current reference to the system being personally controlled and find "My Health Record" to be a bit bland, generic and non-distinct. I'm also not comfortable with the quote in the discussion paper saying "the name of the electronic record should better reflect the partnership between individuals and their healthcare providers" (Clause 3.1.1, Paragraph 31). This comes across as an attempt to water down the patient-controlled aspect of the record and to try to push an "equal partnership" onto patients, usurping their rightful position as the decision makers.

Other

Other issues with the change to an opt-out system include the need for an ongoing information campaign for new patients about this system and the ability for patients to regularly check that they are still opted out. However well you might inform patients at the start of the transition to an opt-out system, in 20 years time, it's much less likely that patients will be adequately informed of the existence of this system and their right to opt out. Likewise, patients who opt out initially may have this changed for them at a later date, perhaps by well-meaning next of kin. What safeguards are

there to protect them from this and to ensure that they are informed if any change to their opted-out status does occur?

In general, patients should be given more oversight over how their medical information is shared, not less. We need more information on every registry, every repository, every portal, every database, every archive, every index, every cloud, every record our data has been sent to and to be given a chance to control that process. One question not addressed in the discussion paper is what the current status is of the legacy state-based ehealth records that existed before the PCEHR? Are they still operational, and do patients know of their existence and their contents?

Summary

In summary, the proposal to change the PCEHR system to an opt-out model should be rejected due to the difficulties many people would suffer in trying to opt out and the sense of violation, humiliation or loss of trust patients may feel at their data being shared online without their consent, or if it gets hacked. Third-party information should not be allowed to be included in PCEHR records, as this removes the right of those third parties to choose not to have ehealth and defeats the whole purpose of personally controlled records.

If an opt-out model is adopted, it should be as easy as possible for patients to opt out, as soon as possible, and leniency should be shown for people with insufficient ID or no fixed address. Patient control should be maintained and expanded to include blocking emergency access to documents and to completely removing documents from the portal and asking that they not be retained. Data retention periods should be shortened considerably, obligated uploads should be rejected, the System Operator should not be granted greater data collection powers, and criminal penalties should only be introduced if patient consent is required to press charges.

Patients should be considered to have exclusive ownership rights over their medical records and should be better informed on how, where and when they are shared and should be notified of all privacy breaches.

H. Nichols