The Information Commissioner's response to the new data security standards and opt-out models for health and social care.

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She also deals with complaints under the Re-use of Public Sector Information Regulations 2015 ("RPSI") and the INSPIRE Regulations 2009. She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) welcomes the opportunity to comment on this consultation, and would be pleased to be contacted by the Department of Health should any further clarification be required. Only those questions relevant to the ICO's remit have been answered.

General Comments – Data Security Recommendations

Recommendation 2 – At paragraphs 1.14 and 2.2.1 the review highlights that data security frameworks, assurance schemes and standards already exist but that there may well be too many pieces of guidance and there is room for standards to be simplified. We would welcome a stronger framework for data security standards and agree with concerns that the IG toolkit can be seen as a tick box exercise. We also have concerns about its potential for unreliable and inconsistent results due to its focus on self-assessment. We would welcome a redesigned toolkit to help embed the new security standards and the recommendations to expand its use are positive. This is a good opportunity to develop a toolkit that could be really beneficial from an information governance perspective as long as its redesign addresses the concerns above.

Recommendation 4 – It would be helpful to include a footnote with a link to information about the Cyber Essentials scheme.

Recommendation 5 – Clarity would be needed around how a contractual requirement for organisations to take account of the security standards would be measured and enforced.

Recommendation 7 – see our comments in relation to question 10 below.

Recommendation 8 – It is essential that the re-designed IG toolkit is fit for purpose, especially given the comments in the review at paragraph 2.2.1 calling for standards to be simplified. Input from the organisations that will be using the toolkit should assist with this. If the redesign of the IG toolkit addresses current concerns around robustness, reliability and inconsistency then it could be a beneficial tool in ensuring data security.

Recommendation 9 – It is not clear what is meant by 'malicious' in this recommendation. It is also not clear whether the harsher sanctions being recommended are in relation to organisations, individuals or both. If greater sanctions are to be introduced then there needs to be greater clarity around what they can be imposed for, particularly what is meant by malicious and who the penalties can be imposed on.

Some security breaches may well result from offences committed under section 55 of the DPA, i.e. knowingly or recklessly obtaining or disclosing personal data without the consent of the data controller. We have set out our position in relation to tougher penalties in relation to s.55 offences in our response to question 12 below.

However, many breaches of the DPA are simply the result of human error. The Commissioner already has powers under section 55A of the DPA to issue Civil Monetary Penalties (CMP's) against organisations for serious breaches of any of the DP principles and she considers these to be an appropriate and effective sanction.

General Comments – Consent/opt-outs

Recommendation 10 – Fair and transparent processing of data is a key obligation within the DPA and key for public trust. Individuals should be made aware through the use of clear fair processing information how their health and social care data will be shared, with whom it will be shared and for what purpose. When sharing data organisations need to ensure that their fair processing information is informative but easy for individuals to understand. However, we often see fair processing

information that is too technical and legalistic and not made easily available. The ICO welcomes the views of the National Data Guardian that the case for data sharing still needs to be made to the public. The provision of clear, coherent and consistent fair processing notices by organisations should assist with making that case.

Recommendation 11 –The ICO welcomes the National Data Guardian's recommendation for a new model of consent in relation to the sharing of patient's medical data. Taking this forward will require care and establishing the correct level of transparency and patient control will be paramount. We acknowledge that introducing an 'opt in' system in this area would carry significant practical difficulties and that an 'opt out' model may be seen as more desirable for a number of reasons. The approach will need to reflect patient expectations and what they may legitimately assume will happen to their data and areas where they would not and may take exception. Whichever model is used, being clear and transparent with individuals about what is happening with their personal data and why is important. This is particularly important for two reasons. Firstly, individuals should be able to understand clearly where they have a choice in relation to the sharing of their personal data and where they do not, such as where the data sharing is required by law. Secondly, it is important because individuals will not be able to make fully informed decisions about what they want to happen to their personal data if the nature of the processing and the implications of their decisions are not clearly explained to them.

It is also important to note that, under the DPA, where personal data is required to be shared by law there are already existing provisions, both in terms of exemptions and schedule conditions, which would cover the sharing of personal data without the need to rely on consent.

Recommendation 12 – Even though HSCIC's name change to NHS Digital may emphasise to the public that they are part of the NHS family, for DPA purposes they would still be a separate data controller. See further comments below at question 11 in relation to point 7 of the 8 point model.

Recommendation 13 – See comments in relation to question 12 below

Recommendation 15 – Organisations and the public need to clearly understand that any explicit consent obtained would be through an alternative method to the opt-out model.

Recommendation 16 – The ICO would welcome this clarification as the current situation around invoice validation appears to be rather confusing, based on the work we have undertaken in this area.

Finally, we wish to make some general comments in relation to points made within the review but outside of the recommendations. At paragraph 1.32 reference is made to health and social care integration and that the review has sought to complement rather than conflict with what is being achieved locally across the country. We are aware of the positive work being undertaken across health and social care integration and whilst we appreciate the scope of the model is limited, we wouldn't want it assumed that integrated care is working perfectly. In our view there are still improvements to be made in relation to data sharing for direct care, especially around improving transparency and fair processing.

Paragraph 3.2.22 refers to the confusion about the law in relation to confidentiality and suggests that the ICO and IGA work together jointly to make the relationship between the DPA and the Common Law Duty of Confidentiality clear for local practice including social care. We would agree that the requirements under the two are often confused. The ICO already works closely with the IGA on certain topics and we would be happy to continue doing this.

Security Standards

6 By reference to each of the proposed standards, please can you identify any specific or general barriers to implementation of the proposed standards?

Please provide your views about these standards.

1. **All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.**

Under the DPA there are eight principles that organisations should follow to comply with the Act. This standard very much links in with some of those eight principles and helps to strengthen some of the requirements within them. We would see no barriers to implementing this standard given that organisations should already be doing this to comply with the DPA.

2. **All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.**

It is important that staff do understand their responsibilities regarding information handling. One of the main cultural barriers we see to data sharing is the risk averse culture that has developed amongst staff and management which includes a fear of losing their jobs for getting it wrong. It is important that this standard is balanced correctly so as not to promote this risk averse culture further and prevent information being shared for fear of getting it wrong.

It should be clarified what is meant by "personal accountability." Under the DPA it is the data controller that is responsible for breaches, so it is important to be clear what, if any personal accountability exists. It is also important to be clear about what is meant by "deliberate and avoidable breaches."

3. **All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.**

It is not clear what will be deemed as appropriate security training and what the mandatory test will include. It is also important that both are consistent across the sector, which we note the review also highlights. Staff training is essential to ensure they have the required knowledge about data security and to comply with the DPA. This standard will help to promote that and assist with embedding IG further within organisations. It is good that the review refers to the annual training being role appropriate with bespoke additional training for those in leadership roles such as Caldicott Guardians, SIRO's and board members.

4. **Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.**

Again, role based access is something that the ICO promote as a security measure in ensuring compliance with the DPA. This is particularly where organisations used large shared databases such as those across integrated care. We would agree that only the appropriate staff should have access to the information and any information accessible to them is no more than they are required to see. We would also agree that all

access to personal data on these systems can be attributed to individuals for audit purposes. The majority of the organisations we have worked with across health and social care seem to be implementing this as part of their integrated care records already, however this standard should help to promote this further.

5. **Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.**

This could be a challenge for some organisations to implement due to resource constraints across the sector. However, this would be a beneficial learning exercise and one which could help to shape future training sessions based on highlighted gaps and weaknesses in processes. Consequently the Commissioner would welcome such a standard.

6. **Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.**

It would be helpful to include a footnote with a link to information about the CareCERT security advice.

7. **A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.**

The ICO would welcome this standard. It is important that lessons are learnt from the suggested annual review and audits.

8. **No unsupported operating systems, software or internet browsers are used within the IT estate.**

It is not clear if there will be any kind of timescale or deadline for this to be achieved. The cost implications could be quite significant for organisations if this is not nuanced correctly. Other challenges might also be in relation to mobile phones and tablets. It could be argued that the majority of smart and feature phones are not supported by the manufacturers. Does this mean that all basic mobile phones, pagers and fax machines need to be replaced?

It would also be good to see a commitment to keep "operating systems, software or internet browsers" up-to-date with patches from manufacturers and software developers.

9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Again the ICO would welcome this standard and that lessons are learnt from the suggested annual review.

10. Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.

Where a data controller uses a third party supplier to process data on its behalf then Principle 7 of the Act requires a data controller to have a written contract in place with any data processors it uses. The written contract should require the data processor to take the same security measures the data controller would have to take if it were processing the data itself. However under the DPA it is the data controller (and not the data processor) that will be held responsible if there was a breach of the Act caused by the data processor. It is worth noting that data controllers may well put liability/accountability clauses within the contracts required by principle 7 however this currently falls outside of our remit. The Commissioner would therefore welcome the addition of this as a security standard which should help to strengthen data security further when using data processors.

If suppliers are to be held accountable by contracts then we presume that the contracts will need to be legally binding. This is something that organisations may require legal advice upon.

It is also worth noting here that the accountability of data processors has been identified as an issue at European Union level and the European Union General Data Protection Regulation (GDPR) will require some accountability in relation to the data processor once implemented. Whether the GDPR is implemented in the UK or not will depend on the government's decisions upon exiting the European Union. It may be worth considering how this standard would interact with the relevant sections of the GDDPR.

7 Please describe any particular challenges that organisations which provide social care or other services might face in implementing the ten standards.

Please provide your views about these standards.

All the comments we have made above would apply equally to both health and social care.

However one additional comment we have is that systems that social care organisations use may be significantly different to the traditional NHS systems. Whilst some of the standards may be fairly straightforward to implement in settings using standard NHS systems, it may be more difficult for social care organisations to achieve the standards.

10 Do you agree with the approaches to objective assurance that we have outlined in paragraphs 2.8 and 2.9 of this document?

◉ Yes

Please comment on your answer.

It is likely that we would amend our audit controls to reference the new security standards. If the CQC is to have a major role in obtaining assurance around the new data security standards then we will need to engage with the CQC and consider whether it is appropriate for the CQC & the ICO to work together. In relation to paragraph 2.9 the ICO would welcome the approaches suggested.

Opt-out model

11. Do you have any comments or points of clarification about any of the eight elements of the model described above? If so please provide details in the space below, making it clear which of the elements you are referring to.

1. You are protected by the law – This complements the DPA as personal data should only be processed in ways that are compliant with the principles of the DPA.

2. Information is essential for high quality care – The ICO has done a considerable amount of work in relation to promoting necessary and justified data sharing across health and social care and assisting organisations understand the legal position when they come up against

perceived barriers. However it is important that organisations understand that when sharing information for care purposes they still need to comply with the principles of the DPA. The suggested opt-out model should not be misinterpreted as allowing organisations to share information in ways that would not otherwise accord with the DPA or any other law.

4. You have the right to opt-out. - As mentioned above in general comments, the ICO welcomes the recommendation of giving patients better control over what happens to their information and an opt-out model within health and social care will be important an method of achieving this. As we have made clear in our comments on Recommendation 11 any approach will need to reflect patient expectations and what they may legitimately assume will happen to their data and areas where they would not and may take exception. Deciding on the manner of expressing a choice will need to reflect the expectations and consequences.

It is good to see that individuals will have an element of choice in relation to their personal information that is shared for non-direct care purposes. While arguments exist for both two separate opt-outs and a singular opt-out, we would point out that the added granularity provided by offering two separate opt-outs would allow individuals more control over how their personal data is used.

That said, however, it is vitally important that the model is clear and easy for both individuals and organisations to understand, especially given the current confusing landscape of multiple opt-outs as outlined in the review. It is also important that the model is one which can ensure that the individual's choices can be honoured consistently across the care systems. Whilst there is no specific requirement laid down under the DPA to offer opt-outs/opt ins other than as part of the means of addressing the DPA's fair processing requirements, DPA breaches can occur where opt-outs are offered and not honoured. This would have principle one implications in terms of fairness, and would also have a detrimental effect on public trust and confidence. That is why it is essential that any model is carefully thought through before being implemented with the right level of choice given at the right time.

It is essential that organisations clearly understand that this is an opt-out model and do not misinterpret a failure to opt out as consent. Where an individual does not choose to opt-out, this is not to be considered as adequate consent for DPA purposes. If an individual does not opt-out, an

organisation will still need a legal basis and appropriate schedule conditions for processing the data for these purposes.

5. This opt-out will be respected by all organisations that use health and social care information. – It is stated that patients will only need to state their preference once and it will be applied across the health and social care system. There are multiple systems across health and social care and some integrated care projects we have worked across have already highlighted issues with interoperability across the systems. It is therefore unclear at this stage how this intention will be reflected and implemented across all systems and honoured by all relevant organisations. We would have concerns that the systems would not talk to each other and this impaired interoperability of systems would make this very difficult to achieve and honour. As mentioned above it is essential that any choices offered can be honoured as failure to do so would breach principle one of the DPA.

6. Explicit consent will continue to be possible. – As commented above, organisations and the public need to clearly understand that any explicit consent obtained would be through an alternative method to the opt-out model.

7. The opt-out will not apply to anonymised information. – We have a few comments in relation to this point. Firstly, we are concerned about the reference to data being passed from NHS organisations to HSCIC, as the statutory safe haven, to de-identify or anonymise the data. It is stated that the anonymised data can be shared with those that need it and in due course, the opt-out should not apply to any flows of information into the HSCIC (particularly paragraphs 1.34 and 3.2.31). We understand that the HSCIC has powers to collect information where it has been directed to do so by the Secretary of State or NHS England, but this is not going to be the case in all circumstances and it is not a general power to collect any information from any organisation. The review seems to imply that all information can be passed to HSCIC to de-identify/anonymise. For the purposes of the DPA, NHS organisations and HSCIC are separate data controllers. This means that NHS organisations need a clear legal basis and schedule conditions to share personal data with HSCIC, even if that data were to be anonymised after it was shared. This may not be the case if the intention is for HSCIC to act as a data processor, but whether this is indeed the intention, is not clear. If it was the intention then care would have to be taken to restrict any further processing of the data by HSCIC. This also appears to be a significant

change to current arrangements, where, for example, the "Type 1" objection allows individuals to opt out of their personal data, held by their GP, being shared with HSCIC. Any increased restriction in the choices available to individuals should be carefully considered and clearly justified.

Secondly, anonymisation can be quite a complicated area and we have concerns in relation to the definitions and terminology being used across health and social care. We note that paragraph 3.2.26 makes the distinction between de-identified data and anonymised data, stating that the previous review described two types of data *"(i) de-identified data for limited access and (ii) anonymised data for publication."* The ICO's Anonymisation Code of Practice (AcoP) defines anonymised data as data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place. The code does not explicitly define de-identified data but it does describe pseudonymised or de-identified data as being one type of anonymised data, which has been anonymised using a particular technique. The definition of de-identified data in the glossary to the review says *"there are two categories of 'de-identified data'; De-identified data for limited access and anonymised data for publication."* This is different to what is said at paragraph 3.2.36, as highlighted above. In addition, we are concerned that the further sub-defining of a term which, in the Anonymisation Code of Practice, is itself a sub-type of anonymised data is likely to lead to confusion. It is important that definitions across the sectors for anonymisation, anonymised data, pseudonymisation and de-identified data are consistent.

Finally, we would agree that the opt-out should not apply to anonymised data i.e. data that does not identify individuals and where identification through its combination with other data is not likely to take place. However we have a number of concerns with the point at Paragraph 1.38 which states that data that has been de-identified according to the ICO's anonymisation code of practice should not be subject to the opt-out. We have already commented above that de-identified data and anonymised data are not the same thing. Only personal data that is 'anonymised' will fall outside the scope of the DPA. This is important as it means that where organisations are processing anonymised data they no longer have to comply with the principles of the DPA, as they would if processing personal data. The key point for data to be anonymised for DPA purposes is the risk of identification. The DPA accepts that the risk of identification does not have to be completely eliminated, an organisation should be able

to mitigate the risk of identification until it is remote. However, if the risk of identification is reasonably likely then the data should still be regarded as personal data. Therefore if the risk of the de-identified data being re-identified is reasonably likely then it would be regarded as personal data and the opt out should still apply.

In relation to it being de-identified "according to the ICO's anonymisation code of practice," we welcome the comments in recommendation 14 around organisations being reminded of the need to have regard to the Anonymisation Code of Practice. However, more generally the code is not a statutory code and was never designed to be a standard for anonymisation. It was not drafted with a view to it being held up as something that 'must' be complied with or that, if it was complied with, was a sign that the data 'was' anonymised. It is designed more as a code for helping data controllers to manage data protection risk and suggests processes they could adopt to help them reach a point where they are satisfied to an acceptable level of risk that the data are anonymised. It is also not specific to the health and social care setting as the ICO does not produce sector specific guidance. Subsequently, the code was designed to be quite broad in relation to the range of processes and techniques that can be used to anonymise data, depending on varying circumstances across sectors and the re-identification risk. In line with our comments above there may be circumstances where de-identified data may still be considered personal data, but there may well be circumstances where the risk has been mitigated enough until it is remote and therefore considered anonymised data. The ICO's view is that the risk associated with de-identified data is extremely broad and whether it is 'anonymised' will depend on varying factors and circumstances. It should be clear that the opt-out will not apply only where data has been 'anonymised.'

8. The opt-out will not apply in certain exceptional circumstances. We have concerns about the significant number of legal requirements to share personal data within the health and care sector. Given this number, this caveat could in fact be extensive and would need to be clearly communicated to individuals so they understand that even when they opt out, their information may still be shared in these exceptional circumstances. Giving choices should be meaningful and not illusory.

12 Do you support the recommendation that the Government should introduce stronger sanctions, including criminal penalties in the case of deliberate re-identification, to protect an individual's anonymised data?

Please comment on your answer.

The Commissioner welcomes the views of the National Data Guardian that there should be strong penalties, including criminal sanctions, for deliberate re-identification. The Commissioner has long made the case for custodial sentences to be introduced for offences under section 55 of the Data Protection Act. The mechanism for this already exists on the statute books under section 77 of the Criminal Justice & Immigration Act 2008. If this were to be brought into force and, if necessary, extended to ensure it clearly covered activities such as re-identification, it would provide a strong deterrent.

The Commissioner is also concerned that a failure to bring in these sanctions could, following the findings of the Advocate General of the Court of Justice of the European Union (the CJEU) in the case of Secretary of State for the Home Department v Tom Watson & Others,[1] weaken the existing data protection regime. In his opinion, the Advocate General suggests that prolonged retention of communications data is permissible only for the purposes of investigating serious crimes. In the UK, a serious crime is that which can result in a prison term of 6 months or more. Since section 55 offences currently carry no custodial sentence, the Commissioner would effectively lose her ability to access communications data when investigating possible section 55 offences. This would severely restrict the Commissioner's ability to investigate and prosecute those involved in the activities of illegally obtaining and disclosing personal data. Whilst it is not guaranteed that the CJEU and the UK courts will follow this opinion, this seems highly likely based on past experience. This underlines the need for the immediate implementation of s.77 of the Criminal Justice and Immigration Act 2008.

15 What are your views about what needs to be done to move from the current opt-out system to a new consent/opt-out model?

What are your views about how the transition from the existing objection regime to the new model can be achieved?

The existing objection regime offers the type one and two opt-outs with the addition of other multiple opt-outs across a number of different settings. From an organisational perspective bringing all that together into one opt out model is going to be quite a challenge and as mentioned above will require significant consideration. The opt-out preference will need to be visible across all systems and settings for all organisations

[1] Joined Cases C-203/15 and C-698/15 http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=96721

across health and social care to honour it. Again, as highlighted above, the interoperability of systems across health and social care could be a significant challenge here.

Staff awareness will also be an important factor in implementing the model successfully as it is likely to be the staff on the ground communicating with the patients that will be implementing these opt-outs. Staff training will therefore be essential and the model will need to be simple for them to understand and implement. The review makes mention of workarounds being used where processes are complicated to get the job done and this being a contributing factor to breaches. If the opt-out model process is complicated or time consuming then there is a risk that this workaround situation could occur here. Organisations will also need to think how the new model will be clearly explained to the public.

From the perspective of the public and patients then fair processing and public awareness is essential. It is important that it is easy for them to understand and make an informed choice. Whichever model is decided upon, it will need to be clearly explained to the public what the opt-out means and when it will, and won't apply. It should also be made clear to the public what channels are available for them to opt out. A key issue will be whether existing opt-outs under the current will remain available under the new model. If existing objections do remain available, then consideration must be given to whether they will be able to be "carried over" to the new system, or whether individuals would have to re-confirm their preferences under the new model. Either way, this will need to be clearly communicated to the public. This is especially important for those individuals who have opted out under the current system in a way that will no longer be available under the new model.

One area of concern here is the recommendation within the review that in due course the opt-out should not apply to all flows of information into the HSCIC. This appears to be a removal of the current "Type 1" objection where an individual can object to their information held in their GP record being shared with HSCIC. The fact that this objection would no longer be honoured would need to be made clear to the public, in particular to all those individuals who have already registered this objection. Organisations would also need to be aware in this instance that any information shared with HSCIC would still need to be necessary and justified, and compliant with the DPA.