

## Schedule L – DPIA0007 – PCN Analytics

### Regional Health and Social Care Information Sharing Agreement

---

#### Schedule L – DPIA0007 – PCN Analytics

This schedule to the Regional Health and Social Care Information Sharing Agreement provides key questions covering six risk categories which when answered objectively offer an initial assessment of the additional risks to privacy posed by the proposed sharing of information.

Where a question gives rise to an affirmative answer, it does not automatically follow that a full scale Data Protection Impact Assessment is required. Each affirmative answer needs to be assessed for materiality (probability and impact) and for ways in which the potential risks can be avoided or materially mitigated with a revised solution or additional measures.

Where a substantial number of questions give rise to an affirmative answer this is a good indicator that a full scale Data Protection Impact Assessment is required and project plans should include the costs and timescales of this activity and any associated consultation that may be needed.

Wherever practical the rationale for an answer should be included with the answer concerned.

*Questions relating to “identity risk” (questions 2 to 8) are of heightened importance in the context of data that has not been anonymised or pseudonymised.*

These questions have been revised to include latest (summer 2018) guidance provided by the Information Commissioner’s Office. Other aspects are based on guidance from the Information Governance Alliance.

#### Technology Risk

1. Does the proposed change apply new, innovative or additional information technologies that have substantial potential for privacy intrusion? ... **Yes. However, the core new technologies have been tried and proven over several years and access to the technology is controlled by strict role based access controls and security and audit measures.**

#### Identity Risk

2. Does the proposed change involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes? ... **No. While datasets will all be identifiable and linkable using NHS Number this policy is in regular use in health and social care. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
3. Does the proposed change have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? ... **No – The existing approach already requires identifiable data to link datasets. Only anonymous and pseudonymous data is made available for viewing.**
4. Does the proposed change combine, compare or match data from multiple sources in a manner that can be used to identify data subjects? ... **No. Data is matched as normal using the NHS Number as required by the 2015 Act.**
5. Does the proposed change include the processing of biometric or genetic data that can be used to identify data subjects? ... **No.**
6. Does the proposed change result in the processing of data concerning vulnerable data subjects? ... **Yes. However, the purpose of the processing includes improving the quality of care and safety of vulnerable data subjects.**
7. Does the proposed change result in the processing of personal data which could result in a risk of physical harm in the event of a security breach? ... **No.**
8. Does the proposed change have the effect of systematically monitoring a publicly accessible place on a large scale? ... **No.**

#### Automation and Profiling Risk

9. Does the proposed change include profiling on a large scale? ... **Yes. As provided by General Data Protection Regulation: Article 6(1)e “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”; and Article 9(2)h “processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”. However, patient processing opt-outs are taken into account and patients who have opted-out from processing are excluded from the processing.**
10. Does the proposed change include evaluation or scoring? ... **Yes, as set out in 9 above.**

## Schedule L – DPIA0007 – PCN Analytics

### Regional Health and Social Care Information Sharing Agreement

---

11. Does the proposed change include automated decision-making with significant effects? ... **No. All decision making is directly supervised by health and social care professionals.**
12. Does the proposed change include systematic and extensive profiling or automated decision-making to make significant decisions about people? ... **No.**
13. Does the proposed change include processing children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? ... **No.**
14. Does the proposed change include profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit? ... **Yes. The proposed change includes processing of special category data to identify data subjects requiring health and social care services and to plan and manage the services for the data subjects concerned. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
15. Does the proposed change include processing involving preventing data subjects from exercising a right or using a service or contract? ... **No.**

### Organisational Risk

16. Does the proposed change involve innovative organisational solutions? ... **No.**
17. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? ... **No. The organisations concerned have considerable history of working together in planning and managing the provision of care. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
18. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? ... **No. The chosen suppliers are long-standing suppliers in the field and have extensive experience with similar data.**
19. Are new processes and relationships required to manage issues with the technology solution and with the accuracy, consistency and completeness of the shared information? ... **Yes. This is an extension of previous sharing arrangements and the core technology is tried and proven.**

### Data Risk

20. Does the proposed change include processing of special category data on a large scale? ... **Yes. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
21. Does the proposed change combine, compare or match data from multiple sources? ... **Yes. However, while datasets will all be identifiable and linkable using NHS Number this policy is in regular use in health and social care. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
22. Does the proposed change include processing of personal data without providing a privacy notice directly to the individual? ... **Yes. As provided by General Data Protection Regulation: Article 6(1)e “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”; and Article 9(2)h “processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32. Furthermore, patient processing opt-outs are taken into account and patients who have opted-out from processing are excluded from the processing. Privacy and processing notices are published by all sharing and user organisations involved in the Regional Health and Social Care Information Sharing Agreement.**
23. Does the proposed change include processing of personal data in a way which involves tracking individuals’ online or offline location or behaviour? ... **No.**
24. Does the proposed change include systematic processing of sensitive data or data of a highly personal nature? ... **Yes. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
25. Does the proposed change include processing on a large scale? ... **Yes. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**

## Schedule L – DPIA0007 – PCN Analytics

### Regional Health and Social Care Information Sharing Agreement

---

#### Exemption and Exclusion Risk

26. Does the proposed change include processing of criminal offence data on a large scale? ... **No.**
27. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? ... **No.**
28. Does the proposed change’s justification include significant contributions to public security measures? ... **No.**
29. Does the proposed change involve systematic disclosure of identifying data to, or access by, third parties that are not subject to comparable privacy regulation? ... **No.**

#### Summary of the Initial Data Protection Impact Assessment

The answers to the above risk questions indicate that a DPIA: *is required / ~~is not required~~* (delete as appropriate).

A previous Initial Data Protection Impact Assessment, which was answered objectively, identified a number of risks requiring mitigation and consequently a full DPIA was conducted.

**A new DPIA has not been conducted as the existing assessment (DPIA0002) is considered appropriate and up to date.**

#### End of Schedule L