NIGB

NIGB response to the Cabinet Office Consultation 'Making Open Data Real'

The National Information Governance Board (NIGB) is an independent statutory body established to promote, improve and monitor information governance in health and adult social care. The NIGB provides advice on the appropriate use, sharing and protection of patient and service user information. The NIGB also advises on the use of powers under Section 251 of the NHS Act 2006 and its associated regulations to permit the duty of confidentiality to be set aside, where other legal routes are not available.

Information governance is the term used to describe the principles, processes, legal and ethical responsibilities for managing and handling information. It sets the requirements and standards that the NHS needs to achieve to ensure it fulfils its obligations to ensure that information is handled legally, securely, efficiently and effectively.

The NIGB regards information governance as essential for the lawful and ethical use of patient and service user information both for the benefit of the individual to whom the information relates and for the public good.

Key considerations

As this is a long and detailed consultation, we felt it important to provide a summary of the key considerations, not all of which may have been included in the responses to the questions asked. These are:

- It is important that the demand for data does not distort the priorities of organisations delivering services. The requirement to publish data cannot be to the detriment of statutory and other functions or organisational priorities.
- Similarly, the collection of data from individuals must only be what is required to deliver services to the individual and not what is desired by researchers and business analysts. Collection of additional data for other purposes must only be with the explicit consent of the individual, both for the use for these other purposes and for any disclosures.
- Organisations and the proposed Public Data Corporation also need to be mindful of the risk that publication of detailed data could become identifiable because of the multiplicity of data sets available (the "jigsaw" effect) either now or in future. A Strategic approach to publication would be helpful to mitigate this risk. This should include consideration of the frequency of publication as data that is published more frequently is more likely to include small numbers that in turn carry greater risk of identification.

- The Consultation document describes the Hospital Episode Statistics (HES) Database as containing non-personal data. Whilst the published statistics from HES are anonymised, the database itself contains identifiable patient data. It is important to acknowledge, therefore, that raw data will often be personal data, albeit that the published outputs must be anonymised.

- We recommend that consideration be given to a "closed data license" modelled on the Hospital Episode Statistics (HES) data sharing agreement for approved researchers where person level data is needed as often there will remain a risk of identifiability for some individuals' data. The license would set out the terms under which they could use the data including what linkage work could be undertaken and disposal and publication arrangements.

- There is a lack of understanding regarding information rights that already exist both for personal data, through subject access under the Data Protection Act 1998, and for official information through the Freedom of Information Act 2004 (FOIA). Improving public and organisational understanding should be addressed before considering strengthening legislative provisions. Additionally, merging the rules relating to FOI and Environmental Information Regulations requests would also be helpful for organisations charged with implementing these different regimes. The ICO is already looking at how to integrate the range of Information Rights.

- Any change to strengthen the "right to data" must also be balanced with ensuring that there are robust safeguards for privacy of personal data. We recommend that serious consideration be given to monetary penalties being applied to failure to respond appropriately to FOI and Subject Access Requests or to respond within the appropriate timescales.

- The consultation includes a proposal to introduce corporate responsibility at Board level to ensure that the "right to data" is being met, using the Caldicott Guardian model. It is not clear whether the intention is to use the Caldicott Guardian model to apply to other sectors or if the intention is to introduce another set of functions at Board level. If the latter, this appears to be based upon a misunderstanding of the role of the Caldicott Guardian, which is to make decisions balancing the public interest in favour of disclosure, or in this case publication, with the public interest of protecting personal and confidential data. In the context of Health and Social Care therefore this "right to data function is already fulfilled by Caldicott Guardians.

- In relation to the concept of charging for data, whilst the NIGB understands the need to recover costs where data is to be processed to extract, cleanse and de-identify it. However, it is also important that the public does not perceive this to be profit-making. Some individuals are likely to be concerned about the commercial exploitation of their data and many people still feel a

sense of ownership of data, especially their confidential information, even when it has been thoroughly anonymised. It also needs to be remembered that a legal basis is needed to process personal data in order to de-identify it and therefore consideration needs to be given to how to manage objections to the use of personal data for secondary purposes which are not statutorily mandated.

- The NIGB would support the proposal that publication of data should be accompanied by a statement of quality and explanation provided to support public understanding of the meaning and uses of such data.

Responses to Specific Questions

1) Do the definitions of the key terms go far enough or too far?

The key terms listed are generally suitable and contain an appropriate level of detail. The definition of the term 'Public services', however, does raise issues. The consultation document refers to providers who have been commissioned or funded by statute as 'public bodies' for the purpose of the consultation. However, public bodies do not include third sector individuals or organisations providing services on behalf of a public body. They are not generally Data Controllers, but Data Processors and, therefore, not legally responsible for determining the use of the data, including disclosure to the public.

The NIGB is of the view that referring to commissioned providers as public bodies is misleading and suggests that a further key term be added 'Contracted out public services'.

2) Where a decision is being taken about whether to make a dataset open, what tests should be applied?

The NIGB proposes the following tests:

- Whether the release of the data would be in the public interest (this is not the same as of interest to the public).
- Whether the public interest justification is sufficient to warrant the work involved in the preparation and publication of data but also balanced against the work involved in responding to FOIA requests.
- Data quality checks to test the integrity of the data and to support consideration of whether it is worth publishing the data; and if so, whether a “health warning” about the quality of the data should be issued alongside it.
- The scale and range of the data source / raw data and whether any individuals could be identified from it. It should be noted that personal data has a broad definition and that there is a risk attached to person level data and aggregate data involving rare occurrences. For example, the consultation

document describes the Hospital Episode Statistics (HES) database as non-personal data. Whilst this is true in relation to published outputs from HES, the database itself includes personal data. Whilst it does not include name and address, the combination of other data items could easily be used to identify individuals if released.

- Analysis with other published datasets to ensure that, by combining datasets, individuals could not be identified. A strategic approach to the overall publication of data sets is needed to optimise the data made publicly available whilst also protecting the identity of individuals.
- Ease of interpretation of the data, to ensure it is not ambiguous and can be clearly understood by the public or whether an accompanying statement is needed.
- The possible manipulation of the data to enable the public to compare 'like for like' results. Has the data been collected consistently using the same data standard, underpinned by a data dictionary? Additionally, whether the data provides a true picture. For example, in the health context, data about individual physicians may not accurately reflect their ability, as individuals at the top of their field, are often sent the most difficult cases and consequently may appear to have poorer outcomes than those of their colleagues. In some instances it may be possible to provide data that conveys an indication of "value added" care for seriously ill patients but in many instances it will be impossible to measure this. If such data were to be published it could result in patients not wishing to be treated by a clinician because of apparent poor outcomes, which do not reflect the clinician's ability. It is also important to avoid circumstances where clinicians could become reluctant to treat patients with poor prognoses to avoid negative impact on their published results.

- Consideration of the audience for the data and in what format it should be made available i.e. data would be presented differently for the public and for researchers.

3) If the costs to publish or release data are not judged to represent value for money, to what extent should the requestor be required to pay for public services data, and under what circumstances?

If release of the data is not deemed to be value for money, then this on its own is not justification for making a charge or withholding the data. The issue of charging should only arise where the data does not already exist in a suitable format for publication and would need significant work to be extracted, sorted or converted into a suitable format for the requester to be able to interpret it correctly. The approach to charging needs to take account of Freedom of Information requirements.

4) **How do we get the right balance in relation to the range of organisations (providers of public services) our policy proposals apply to? What threshold would be appropriate to determine the range of public services in scope and what key criteria should inform this?**

The NIGB considers that, although the policy proposals should apply to all public services, responsibility for decisions relating to the publication or release of the data must rest with the public body who has commissioned the service(s). This is because, in general, the public body will remain the Data Controller for the personal data used to generate the published (anonymised) data. This is also in line with its responsibilities under the FOIA and EIR. The Data Controller has responsibility for the confidentiality, integrity and availability of the data.

Where a public body has commissioned or contracted out a service to a third party individual or organisation, that body is a Data Processor, whose information governance responsibilities are determined under contract with the public body.

The public body, as data controller, will need to set out in contract what data should be collected and recorded by the commissioned provider, including the frequency of collection and in what format it should be submitted to the Data Controller. The Data Controller will need to verify the data before considering whether it should be published.

The commissioned provider should not incur additional costs not covered under contract, so it is important that data requirements are made clear at an early stage, ideally in the tender documentation.

Any proposals need to align with FOI and EIR. Organisations that are not subject to FOI or EIR should not be included in scope. These Acts only apply to public bodies. Only the DPA and Human Rights Act apply to all organisations that process personal data.

5) **What would be appropriate mechanisms to encourage or ensure publication of data by public service providers?**

There would need to be mandatory datasets for publication, for example, public authorities must currently publish expenditure over £500. An appropriate mechanism would be the Freedom of Information (FOI) Act. However, there is currently confusion as to the classification of FOI and Environmental Information Regulations (EIR) requests. In our view, it would be beneficial for them to be brought together with a single set of rules and exemptions.

Public bodies are reliant on the functionality provided by their IT systems to collect data and run reports in a format that is suitable for publication. To avoid the public having to search each public body's website for data, there should be a single data portal, such as through direct.gov.uk, to which each organisation could export their

data. The government is proposing such a single portal in their proposal for a Public Data Corporation (PDC).

Data and Information standards and interoperability guidelines will need to be made available to ensure 'like for like' data is published within the PDC. Public bodies should include on their own website a link to their information published on the PDC so that people can go directly to that organisation's published data and be able to compare it with the same data sets published by other bodies.

Publication of 'like for like' data may necessitate IT upgrades to ensure that the desired data can be produced and in an appropriate format. Consideration should be given to central government funding for these upgrades.

Policy Challenge Questions

1) An enhanced right to data

a) How would we establish a stronger presumption in favour of publication than that which currently exists?

The NIGB takes the view that there is already a strong presumption in favour of publication through Freedom of Information; in particular through the requirements of the model publication scheme. It may be that this would benefit from further amendment to encompass not only what is currently published under the FOIA and EIR, but with a wider remit, to include both mandatory and desirable datasets for release. The NIGB is aware that the ICO is consulting on its Model Publication Scheme, so the timing would seem appropriate. It may also be that consideration should be given to further enforcement mechanisms for the ICO such as fines for failures to publish or disclose information where appropriate under the FOIA.

Having said this unless publication is mandated, organisations are unlikely to fully comply. This is because all public bodies are operating in an increasingly financially constrained environment and there are often insufficient resources to carry out tasks other than those which must be completed to meet statutory requirements. Good practice alone is unlikely to be enough to encourage organisations to publish anything over and above what is mandated. When considering which data sets should be mandated, careful consideration therefore needs to be given to the burden of work in preparing data for release.

It is important that the collection and publication of data is driven by and supports better outcomes for patients and service users, rather than driven by performance statistics and the desire to be 'top of the table'.

b) Is providing an independent body, such as the Information Commissioner, with enhanced powers and scope the most effective option for safeguarding a right to access and a right to data?

The NIGB supports the view that there should be an independent body and that the Information Commissioner is the appropriate independent body because of the joint responsibility to balance freedom of information with personal privacy. Additionally, the enhanced powers and scope of the independent body need to include the authority to investigate the integrity and validity of the information that will be provided to the applicant or, in the case that the public authority has claimed that the data does not exist, to investigate whether this is the case. This would necessitate providing the independent authority with auditing powers.

The public body (Data Controller) should be asked to submit evidence to the independent body if required and / or allow staff from the independent body to access their data (including the original data source) if considered necessary. This is only likely to occur rarely, but nevertheless is a power that is necessary for the independent body to have.

c) Are existing safeguards to protect personal data and privacy measures adequate to regulate the Open Data agenda?

The NIGB takes the view that existing safeguard to protect personal data are not adequate and they are often not sufficient to regulate existing publication requirements. This is for a number of reasons: the broad definition of personal data is not well understood; effective anonymisation is not well defined; whilst regard is given to compliance with DPA requirements, confidentiality and privacy under the Human Rights Act is not necessarily given due regard or the three sets of requirements interpreted appropriately in their interaction with one another. Additionally, it is important to be aware of the differences in the privacy requirements for personal data about living individuals and identifiable data about deceased persons, for example the DPA only applies to the living but confidentiality, where it has applied in life, in general should be regarded as extending to the deceased[1].

It is likely that the published data will be used for research and secondary use purposes and to analyse trends. In order to validate the integrity of the data for these purposes, checks would need to be made on source data, prior to anonymisation or pseudonymisation or in some instances to verify the data after publication. It needs to be made clear who would have the powers to undertake these checks, and the legal basis for processing personal data for such purposes.

In relation to anonymised or pseudonymised person level data or aggregate data including small numbers, it may be possible, particularly when comparing it to other published data, to identify the individuals.

In order to extract data for a data set, the raw data accessed may be personally identifiable data. In the case of health and social care data, the staff tasked with

[1] Bluck v Information Commissioner, Lewis v Redfern and Secretary of State for Health, Plon v France.

undertaking this work will probably not have a 'legitimate relationship' with the data subject (i.e. not involved in supporting their health or wellbeing). Therefore, the patient or service user's personal and confidential data would be processed both for reasons other than originally intended when the data was collected and disclosed to staff they would not expect to access. Whether the data is being processed for a compatible purpose is open to interpretation and affects which circumstances an individual's personal data can be used without their (further) consent. Even where the purposes are to be regarded as compatible, where this involves a disclosure to staff with whom they do not have a relationship or disclosures of identifiable data outside of the organisation, then this could breach confidentiality and consequently also the first Data Protection Principle.

Access to deceased persons' social care data (not covered under the Access to Health Records Act or the DPA) is not adequately regulated. It is not clear whether any elements of the Human Rights Act continue after death and, if so for how long. Would the same protection be afforded to personal data about deceased persons as to living persons when publishing data relating to deceased persons?

Data Controller and Data Processor roles and responsibilities, particularly in terms of contracted out services, are open to interpretation.

d) What might the resource implications of an enhanced right to data be for those bodies within its scope? How do we ensure that any additional burden is proportionate to this aim?

Additional resource requirements will be high initially, however, as more information is routinely published, it is expected that the volume of FOI and EIR requests would be expected to reduce over time and this would offset the costs involved in publication of the datasets. Whilst this may be true, it is also possible it would lead to new FOI requests seeking further detail.

Any additional burden on the Data Controller will depend on the frequency of submission of data to the Public Data Corporation (PDC). It will also depend on how easily the datasets can be interpreted by the public, the functionality (e.g. search criteria) and navigation of the proposed PDC. If it is not easily navigable, this will not serve to reduce the number of FOI requests received by public bodies.

A wider model publication scheme, in line with new requirement and consistent with the structure of the PDC would help to ensure a consistent and proportional approach.

e) How will we ensure that Open Data standards are embedded in new ICT contracts?

Requirements must be included in tender documentation and evidence of compliance tested during the tender stage. Consideration needs to be given to the protection of personal data as well as to interoperability within both Open Data Standards and ICT contracts.

Model contracts and example clauses should be made available on the website of the independent regulating body. Contract clauses should include a range of Information Governance clauses to ensure the protection of personal and confidential personal data such as the right to audit information governance measures and how data is being processed.

Data Controllers must design methods to monitor compliance and the integrity of data, including data collected from commissioned / contracted out services, who will usually collect and record data on their own ICT systems. As already mentioned, data that is made available to the public must be determined by the Data Controller, and not directly by the contracted provider (the Data Processor).

Data and systems will need to be compatible with the requirements of PDC to ensure interoperability. Users should be able to view comparative local data sets and national or regional data sets in the PDC, with an option to extract the data relevant to an individual public body. A further option could be *'View other datasets published by (name of public body)?'*

2) Setting transparency standards

a) What is the best way to achieve compliance on high and common standards to allow usability and interoperability?

There will need to be approved processes for managing information, and the adoption of Standards is key to enabling cross organisational and cross sector data flows. These Standards will need to be approved by the relevant appropriate bodies, such as the Information Standards Boards for Health & Social Care, and for Education, Skills and Children's Services.

b) Is there a role for government to establish consistent standards for collecting user experience across public services?

Yes, all users, particularly of health services, need to be able to provide feedback, including feedback about particular services and individual members of staff. There are also defined methodologies for ensuring that questions are framed in ways which do not bias the feedback and also to elicit the responsiveness of individuals. Citizens and service users need to be able to feedback easily, in a way that is clear to them and to whoever receives it. Feedback needs to be concise and consistent, and structured so that it can be interpreted by whoever analyses it. It is also important that feedback is used to influence how services are delivered and to address poor practice.

Government needs to provide a list of key items for feedback and these must include information that will improve the user experience and achieve better outcomes. There needs to be an outcome from the feedback – accountability, improvement, and rewards.

Citizens must have the option of feeding back anonymously if they want to.

c) Should we consider a scheme for accreditation of information intermediaries, and if so how might that best work?

It is not clear what is meant by 'information intermediaries'. Examples of what might be included in their role are needed. For example, is it anticipated that these intermediaries would have access to personal data and undertake analyses on behalf of public bodies? Or would they obtain aggregated data and their role be to present it in meaningful ways to members of the public and targeted to different populations? It is essential that any information intermediary has a clear legal basis to access personal data if they are to act as 'agents' who process data into a non identifiable format.

Whoever operates the PDC might be considered an intermediary. A scheme of accreditation might be developed for these operators. Further information is needed before being able to respond to this question fully.

3) Corporate and personal responsibility

a) How would we ensure that public service providers in their day to day decision-making honour a commitment to open data, while respecting privacy and security considerations?

There needs to be a balance between providing services and making data available. The process for making data open needs to be embedded into routine practice.

Data that can be linked to an individual will need to be anonymised or pseudonymised before it can become open data, so this element will need to be included in the process.

Public service providers must acknowledge that they are accountable, for the quality of the services they provide and how public monies are spent (value for money). Accountability requires openness and transparency.

b) What could personal responsibility at Board-level do to ensure the right to data is being met include? Should the same person be responsible for ensuring that personal data is properly protected and that privacy issues are met?

This should be the collective responsibility of Board members, with each member being personally responsible for the data that is processed within their own areas

of responsibility. However, although the Board will have overall responsibility, day to day responsibilities will sit lower in the hierarchy, for example, with information governance officers, records management and FOI officers. These officers should have responsibility for reporting to Board members and attending Board meetings at intervals to report on access to data.

Ensuring that personal data is protected and that privacy issues are met alongside decisions about the publication of data are roles for the same officers, both at Board level and at operational or day to day level.

The responsible board would ideally be an information governance board and membership should include the Senior Information Risk Owner (SIRO) and the Caldicott Guardian, as well as Information Asset Owners, i.e. database owners.

Information governance is concerned with facilitating the safe and lawful use of data through the adoption of appropriate approaches to the use of personal data and systematic safeguards.

c) Would we need to have a sanctions framework to enforce a right to data? What sectors would benefit from having a dedicated Sector Transparency Board?

Any sanctions framework needs to be incorporated into the existing legislative framework and should be balanced with sanctions for breach of privacy.

In addition, since a significant proportion of data is processed outside the EU, consideration needs to be given to the protections afforded by other countries. Otherwise, business is hampered, affecting choice, quality and price.

Given the particular issues faced by the health and social care sectors related to sensitive personal data and the duty of confidentiality that is owed to individuals there is benefit in having dedicated sector specific boards but we consider that these cannot just consider transparency issues but need to consider transparency balanced alongside privacy requirements.

4) Meaningful data

a) How should public services make use of data inventories? What is the optimal way to develop and operate this?

Public services need to make use of data inventories to ensure they are aware of the full extent of the personal and other data for which they are responsible. They should also include the purposes for which data is collected and used and who the Information Asset Owner is.

The NHS already has information asset registers which could be used as the basis for data inventories. Enhancements could be developed and operated through the PDC.

Retention periods for identifiable data need to be defined, so that any historical data that is no longer required is either destroyed or completely de-identified.

Any process must include a review step and adoption of a variety of methods to ensure that individuals cannot be identified from the published data.

b) How should data be prioritised for inclusion in an inventory? How is value to be established?

This question suggests that an inventory is different from an Information Asset Register, in that an asset register is for internal use and would encompass all information assets, whereas an inventory outlines a list of data which is either published or which could be published. In determining which data to make available, consideration needs to be given to which is of most value (e.g. to individuals, commissioners, service providers, the individual public body). This may be for a variety of purposes, as indicated above.

Data that is already published elsewhere would not be a priority. Data that is commonly requested through FOI could be prioritised to reduce the number of FOI requests.

There are some 'quick wins' in relation to data that is already collected, for example, performance data or data that is collected and recorded for statutory purposes.

c) In what areas would you expect government to collect and publish data routinely?

Any areas where the data could help patients, service users and practitioners to make informed choices and decisions would be beneficial. Also any data that would enable benchmarking and target setting, or aid openness and accountability would be useful.

In health and health & social care, there are examples below:

- Waiting lists
- Operations carried out – reason, type of anaesthesia (local, general)
- Death statistics - cause of death, including by area, age, gender etc
- Staffing data – vacancy rates, qualifications
- Costs – staffing, medication, equipment
- Research and analysis for health conditions, including long term conditions and related demographics, e.g. age, gender, disability, ethnicity (again provided it was not identifiable data
- Medications – stock and usage
- NHS Equipment stores

- Birth statistics
- Hospital admissions and discharges
- Public health data – infection, vaccination take up, sexually transmitted diseases, smoking cessation
- Numbers of people in receipt of Council funded support, Continuing Care, Free Nursing Care
- Care home vacancies (with nursing care, without nursing care, Learning Disabilities, Mental Health)
- Numbers in receipt of home care, day care, Meals on Wheels, Community Alarm services,
- Personal Budgets and Direct Payments
- Grants to voluntary organisations and value of outsourced contracts

d) What data is collected 'unnecessarily'? How should these datasets be identified? Should collection be stopped?

It's difficult to know in advance when it would be beneficial to see trends developing or whether data would have any historical value in the future other than for long term outcomes. Any data collection needs to be carried out, with the view that it must serve an identified useful purpose, not necessarily in the short term, but over a period of time.

Any data that is not collected with a view to improving the user experience or better outcomes should not be collected other than where it is an identified proxy for outcomes e.g. HbA1c measurement is not an outcome measure in itself but a well evidenced indicator for good long term outcomes for diabetes.

The DH Fundamental Review of Data Returns has looked at reducing the number of NHS data returns. The NIGB will consider responding to this consultation in November.

e) Should the data that government releases always be of high quality? How do we define quality? To what extent should public service providers 'polish' the data they publish if at all?

Published data must be consistent and of good quality. To ensure this is the case data will need to be verified. In some instances a judgment will need to be made about whether the quality of the data is good enough, or if the quality of the data is such that the data could be misleading and therefore that the balance of public interests would not favour publication as this would potentially give rise to poor decisions. We would recommend that the decisions to publish or not publish data could itself be published with a statement of quality as supporting evidence for the decision.

To ensure consistency and interoperability, data standards are required and these will need to ensure that 'like for like' data is included in any dataset. As explained earlier, some datasets may need to include a value added formula, to ensure results are not distorted.

5) Government sets the example

a) How should government approach the release of existing data for policy and research purposes: should this be held in a central portal or held on departmental portals?

To facilitate ease of access there should be a single point of entry portal for access for the public and researchers to de-identified data. Data for policy and research purposes will often be derived from personal data. It is essential, however, that the data held by a central portal should only be available fully anonymised. It could include links however to departmental or organisational portals which provide a de-identified view of a database which includes personal data but which is not made available outside of the organisation.

b) What factors should inform prioritisation of data sets for publication, at national, local or sector level?

Data related to current issues and priorities.

Public authorities will want to publish data that are likely to reduce the number of FOI and EIR requests wherever possible. They should look at the subject matter and details of requests and, where there are repeated or similar requests for data, publish that data. A high number of requests of a similar nature are a good indication of what members of the public are interested in. Although this would not necessarily achieve better outcomes in any particular area, it would achieve more accountability and transparency, as well as reducing the burden of FOI and EIR requests.

Local residents could be invited to 'have their say' about what datasets are published locally. Similarly, there may be particular stakeholders or population groups nationally which could also be invited to prioritise data for publication.

c) What is more important for government to prioritise publishing a broader set of data, or existing data at a more detailed level?

We are unclear why one might have to be more of a priority that the other. The process of setting priorities will depend on how useful the data will be and / or the level of public interest in the data. As mentioned above, it would be worthwhile gathering data on FOI requests as a starting point. Some of this will be for new data and some for data that is already published, but at a more detailed level. The NIGB would urge caution in relation to more detailed level data where it is derived from personal data as the greater the detail, the more likely the risk that some of the data could lead to identification of individuals.

6) Innovation with open data

a) Is there a role for government to stimulate innovation in the use of Open Data? If so, what is the best way to achieve this?

The NIGB's view is that government has a responsibility to model good practice in making data available and in stimulating innovation. It also has a responsibility to ensure that commercial interests do not take precedence over public interests in relation to making data available e.g. research methodologies and efficacy and safety results for drugs trials at an appropriate point in the licensing process.