



Data-sharing review

A consultation paper on the use and sharing of personal information in the public and private sectors

Northgate Information Solutions' response
February 2008

Data sharing review

1. Northgate welcomes the opportunity to contribute this brief response to the Data Sharing Review.
2. The company is a leading provider of specialist software, outsourcing and information technology services to the human resources and public services markets. Northgate currently employs over 6,000 staff and operates in 46 countries across 5 continents. Northgate has approximately 4,500 large/medium customers and approximately 10,500 small/medium enterprise (SME) customers world wide. Northgate's customers include works approximately 1 in 5 Fortune 500, 90% of the UK local authorities and all of the UK's police forces.
3. Throughout our daily operations we are involved in sharing data. We are heavily involved in the processing of confidential and sensitive personal information for our employees, our clients and our other stakeholders, for example as a provider of payroll services and in the information that we hold at our data centre.
4. Whilst we believe that data sharing can lead to enhanced public services (see below) we, also take the issue of data security as critical to ensuring successful data sharing. For our business, data security is a matter of operational integrity.
5. To ensure stakeholder trust in our integrity, we are adopting ISO 20701 through a process of continuous improvement to critical parts of our business. This enables the company and its customers to benefit from best in class information security management systems.
6. We aim to embed information security throughout the daily operations of the company.
7. The Board holds responsibility for information security management and there is an agreed corporate security policy and security policy and standards, made available on the corporate intranet to all employees.
8. Northgate's policy aims to ensure that information is only accessible to those authorised to have access; that the information that the company processes and its processing methods are accurate and complete; and that the information that is processed is available to all authorised in the right place at the right time.
9. It is the responsibility of Northgate managers to ensure that all Northgate employees, visitors, temporary and contract staff comply with the policy and standards, processes and procedures.
10. An information steering group reports to the board and meets on a bi-monthly basis to analyse risk and to undertake regular information security risk assessments, to share best practice; to promote continuous improvement and to report any actual or suspected breach of the security policies and standards to the Information Security Manager who investigates all incidents.
11. The company provides regular security awareness training to all staff. All new employees learn about the importance of information management through their induction, and an

innovative e-learning course is available for all employees. It is proactively targeted at individuals who have the greatest need.

12. The policy is reviewed, at least, on an annual basis and the Board receives regular reports on its progress.

The opportunities and risks of sharing data

13. All citizens have the right to enjoy accessible and responsive public services, able to deliver sustained improvement to the quality of life. It is fundamental to community well-being.
14. At both a national and local level, the structure of public services has traditionally placed organisational functionality above personal need. The real challenge is to meet citizens' demands for services that are proactive and responsive to individual need, and that keep pace with changing expectations.
15. In the area of public services, there are many benefits for the public in agencies sharing information, particularly in the delivery of personalised services. There is no 'one size fits all' approach to public service delivery; people may choose to access services in different ways, but it is crucial that all services are easily and equally accessible .
16. In the past, people have been let down by the fact that local service providers do not share information in a timely and cost effective manner, have been reactive rather than proactive, and have failed to connect with their communities in delivering permanent change.
17. There is no technological reason why, when a person leaves hospital, for example, the appropriate service deliverers cannot be notified and jointly provide a proactive, cohesive service to meet an individual's requirements.
18. There are, of course, dangers with such an approach. People's civil rights and security need to be protected, and people's nervousness about giving personal information needs to be addressed.
19. There needs to be established clear protocols and rules for shared data. There must be transparency about what information is being shared and why, in order to gain people's confidence that data is being held for a legitimate process and that the information collected is necessary for the purpose.
20. Clear and consistent communications linked to the objective of enhancing the awareness of the importance of information sharing and security in promoting progressive services need to be accompanied by stronger forms of enforcement.

The legal framework

21. We support the principle-based approach of the Data Protection Act.
22. However, our concern is that there generally remains a relatively low awareness of how to apply a principle-based approach to practical situations and to embed this within organisational practice. This can, in our experience lead to a risk-averse approach within and

between organisations in which data which can legally be shared or there can be a low level of awareness about the importance of information security.

16. Given the growth of new technology and the wider availability of information that may be shared, the importance of data security should not be overlooked. In our experience, much more use could be made of technology to protect information. The process of extracting information and select fields from databases is relatively simple and there are a number of off the shelf products which assist in this process. This not only protects information but can provide cost savings to customers.
23. Raising awareness of the application of data protection law and effective information sharing and security is key to ensuring the proper use of data. We do not under-estimate the challenge that this presents.
24. In our experience, greater use could be made of developing interactive tools to assist in this process.
25. We also think that consideration could be given to developing awareness about the issues within the national curriculum, particularly in the context of the citizenship agenda, so that awareness can be built and developed at an early stage of a person's development. Our schools currently provide little information for students on data protection, computer security and information security.
26. There is also a need to consider how data protection issues can be more effectively built into business management courses.
27. Alongside the importance of education and raising awareness, we believe that there are strong arguments for strengthening the current enforcement powers that exist, for example, by introducing custodial penalties for the deliberate and wilful misuse of personal data.
28. In our experience, much more use could be made of technology to protect information. The process of extracting information and select fields from databases is relatively simple and there are a number of off the shelf products which assist in this process. This not only protects information but can provide cost savings to customers.

Further information