HM Government

Data Protection and Sharing – Guidance for Emergency Planners and Responders

Non-statutory guidance to complement *Emergency Preparedness* and *Emergency Response & Recovery*

Published: January 2007

ISBN: 0711504784

Contents

How to use this guidance

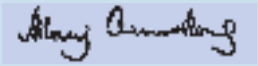
The guidance should be used in conjunction with the non-statutory *Emergency Response and Recovery* and statutory *Emergency Preparedness guidance*. These guidance documents are available on the one-stop website for risk and emergency practitioners – www.ukresilience.info. This guidance is designed to:

- inform Category 1 and 2 responders and other responders (such as those in the voluntary sector) on the key issues relating to data protection and sharing in emergency planning, response and recovery;
- cover the whole of the UK.

If you have any comments about the guidance, or any further ideas about how we might improve or add to it, please contact the Cabinet Office via the feedback form on the UK Resilience website.

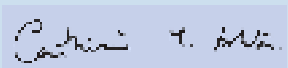
Forewords

One of the lessons identified in the Government's report on lessons from the 7 July 2005 attacks related to the management of personal data by local and regional responders. It was apparent that in some parts of the emergency response, the requirements of the Data Protection Act 1998 were either misinterpreted or over-zealously applied. Subsequent reports from the regions have indicated that the London experience in this respect is not unique. As a result, the Cabinet Office has worked with a wide range of stakeholders across government to develop tailored guidance for the emergency community to dispel some of the myths and provide a useful resource to inform future emergency planning, response and recovery. The guidance is being incorporated into training at the Emergency Planning College. The guidance contributes to the Government's vision for information sharing. Our vision is to ensure that information is shared to expand opportunities for the most disadvantaged, fight crime and provide better public services for citizens and business, and in other instances where it is in the public interest.



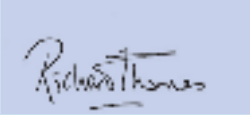
Hilary Armstrong
Minister for the Cabinet Office

The Data Protection Act 1998 is an important piece of legislation giving confidence to individuals that their personal data will be treated appropriately and that it will not be misused. Its job is to **balance** individuals' rights to privacy with legitimate and proportionate use of personal information by organisations. In the context of emergency planning – and, in particular, in the aftermath of an emergency – it is important to look at this balance critically and realistically. The public interest is highly likely to mandate the sharing of information to help both immediately affected individuals and the wider community in such circumstances. Indeed, our view is that emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do *not* share information. We must all work within the law, but in the circumstances set out in this guidance, we feel that uncertainty should not be used as an excuse for inaction when it is clearly in the interest of individuals and the public at large to act positively.



Baroness Ashton of Upholland
Department for Constitutional Affairs

The first of the Key Principles in this guidance makes clear that data protection legislation is not a barrier to appropriate information sharing and provides a framework where personal information can be used with confidence that individuals' privacy rights are respected. This has always been the case but on occasions organisations who want to be certain about their compliance with the law err too far on the side of caution. This can be particularly true where there is little time to consider matters fully or take appropriate advice. This practical guidance helps those faced with making decisions to resolve any uncertainty they may have about what personal information can be disclosed and when. This should help ensure that the twin objectives of appropriate information sharing and necessary privacy protection are properly seen as complementary objectives and not competing ones.



Richard Thomas
Information Commissioner

Chapter 1
Introduction and key principles

Summary

- Background and aims of the guidance (paragraphs 1.2–1.3).
- Scope of the guidance and definitions of 'personal data' (paragraphs 1.4–1.9).
- The legal context of data protection and sharing (paragraphs 1.9–1.13).

Introduction

1.1 In the light of the 7 July 2005 attacks it was clear that emergency planners and responders required additional guidance specifically on data protection and sharing in an emergency.[1] To quote the key report into the 7 July 2005 attacks, the Government's resilience lessons paper noted that:

> *"Limitations on the initial collection and subsequent sharing of data between the police and humanitarian support agencies hampered the connection of survivors to support services like the Assistance Centre. The concern at the time was that the Data Protection Act might prevent the sharing of personal data without the explicit consent of those concerned. As a result, there were delays in information reaching survivors about the support services available. An over-zealous or incorrect interpretation of the duties imposed on public organisations by the Data Protection Act has been previously identified in the Bichard Inquiry as a cause for concern. That inquiry found no reason why, where the sharing of data was appropriate and for a good purpose, it should not be done."*[2]

1.2 This issue is not confined, however, to the 7 July 2005 attacks. Though the challenges were perhaps not as acute, similar problems were faced handling personal data in responding to the Asian Tsunami in 2004 and Hurricane Katrina in 2005. The Victoria Climbié Inquiry of 2003 and the Bichard Inquiry of 2004 also made similar recommendations relating to the handling of personal data.[3]

Aims of the guidance

1.3 This publication does not introduce any new policy or legal requirements. It rather seeks to provide clear and understandable guidance on the legislative framework surrounding personal data so that emergency responders know what they can and cannot do when handling personal data. By exploding some of the myths that have built up around data protection, we will be better placed to prepare for, respond to and recover from emergencies. The guidance contributes to the Government's *Vision for Information Sharing in the Future* published by Department for Constitutional Affairs (DCA) and the Government's *Action Plan on Social Exclusion* published by the Cabinet Office.[4] A comprehensive plan for information-sharing across the public sector is due for publication in April 2007.[5]

Scope

1.4 Key stakeholders who have been consulted in developing this guidance include the DCA, the lead government department for the Data Protection Act 1998 and human rights law, and the Information Commissioner's Office (ICO) as the UK's independent public body set up to promote access to official information and to protect personal information. The Information Commissioner regulates and enforces the Data Protection Act 1998 and the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

---

1 This is principally Category 1 and 2 responders (ie the emergency services, local authorities and certain utility companies). The guidance is also for non-Category 1 and 2 responders involved in civil protection such as the voluntary sector. For a definitive list of Category 1 and 2 responders, see Parts 1 and 2, Schedule 1 of the Civil Contingencies Act 2004 available at: **www.opsi.gov.uk/acts/acts2004/20040036.htm**

2 See the Government's report on *'Addressing Lessons from the Emergency Response to the 7 July 2005 London Bombings'* at: **http://security.homeoffice.gov.uk/news-publications/publication-search/general/lessons-learned**

3 See: **www.bichardinquiry.org.uk/report/** and **www.victoria-climbie-inquiry.org.uk/index.htm**

4 See: **www.dca.gov.uk/foi/sharing/information-sharing.pdf** and **www.cabinetoffice.gov.uk/social_exclusion_task_force/reaching_out/**

5 See the Cabinet Office publication, *Transformational Government: Implementation Plan,* available at: **www.cio.gov.uk/documents/pdf/transgov/transgovt.pdf**

1.5 Other key stakeholders involved in the consultation process were the Home Office (HO), Department of Health (DH), Health Protection Agency (HPA), Department for Culture, Media and Sport (DCMS), Department for Transport (DfT), Foreign and Commonwealth Office (FCO), Department for Communities and Local Government (DCLG), Association of Chief Police Officers (ACPO) and the Local Government Association (LGA). Given the guidance covers the whole of the UK, officials in the Scottish Executive, Welsh Assembly Government, the Northern Ireland Office and Northern Ireland Administration have been consulted.

1.6 Whilst a great deal of information may need to be shared in relation to planning for or dealing with an emergency, only some of this will be personal data. This guidance focuses on personal data because this is where emergency planners and responders have experienced most problems. By 'personal data', we mean data falling within the definition of 'personal data' provided by the Data Protection Act 1998. This can be summarised as:

- information relating to a living individual, from which that individual can be identified, or which can be used to identify that living individual in conjunction with other information held (or likely to be held) by a data controller. Personal data/information includes expressions of opinions about that person, or indications of intent towards them;
- included in this is 'sensitive personal data' which comprises information about an individual's:
  - racial or ethnic origin;
  - political opinions;
  - religious beliefs;
  - trade union membership;
  - health;
  - sexual life; and
  - criminal activity.[6]

1.7 While the nature of an emergency will vary (broadly falling into those that arise from terrorist-related action, other incidents and natural disasters), the principles and legislative basis underpinning the sharing of information are broadly the same. This guidance does, however, highlight where there are differences – in particular in law enforcement-related emergencies where the powers of the police are particularly relevant.

1.8 While the problems arising from information sharing have been most acute during the emergency response phase, sharing of information is critical to all stages of an emergency. The principles and legislative framework explained in this guidance apply to the planning, response and recovery phases – though as is made clear, the balance in either sharing or not sharing information can shift during phases of an emergency. During an emergency it is more likely than not that it will be in the interests of the individual data subjects for personal data to be shared.

Legal issues

1.9 Although different areas of law apply to data sharing – specifically the Data Protection Act 1998, the European Convention of Human Rights (ECHR) Article 8 and the common law of confidentiality – it is important to recognise that there is overlap between them. The particular rules of the various pieces of legislation cannot be ignored. These rules are explained in as non-legalese language as possible in this guidance. When considering the issues and to help get to the right decision in an emergency it is acceptable for responders to have in mind some fairly broad-brush and straightforward questions:

- is it unfair to the individual to disclose their information?
- what expectations would they have in the emergency at hand?
- am I acting for their benefit and is it in the public interest to share this information?

[6] The full legislation can be accessed via: **www.dca.gov.uk/ccpd/dpsubleg.htm**

These suggested perspectives are not a substitute for deciding about fair and lawful processing, whether a Data Protection Act 1998 condition is met or whether a duty of confidentiality applies, but they are useful tools in getting to the right view.

1.10 Inevitably, answers to these questions will depend on the specifics of the emergency in question, such as the personal data that needs to be shared, the reasons why it needs to be shared, and the organisations involved. The broad principles explained in this guidance and the series of case studies at **Annex B** should, however, provide responders with greater confidence to make the right decision. Understanding these broad principles and putting in place processes and agreements before an emergency should help smooth the decisions in the heat of an emergency. For example, when collecting personal data routinely, responders should include a statement that the information may be shared in the event of an emergency situation in which they are involved.

1.11 Following these broad principles in an emergency will mean that the sharing of data is unlikely to be found unlawful. Moreover, responders should also be reassured that if they decide in good faith that it is appropriate to share personal information during an emergency, then they are extremely unlikely to be personally legally liable if – after the event – it turns out that the information sharing was not lawful. In the unlikely event of a complaint or mistake, any action or claim for compensation would almost certainly be made against the organisation concerned (and if not you could expect your organisation to support you).

1.12 Where a mistake is made and information is shared in breach of the Data Protection Act 1998, any enforcement action would be taken against the organisation, not the individual. There is an offence under the Data Protection Act 1998 if an individual knowingly or recklessly discloses personal data without the consent of the data controller (organisation). But this need not concern a person making data protection decisions in the course of their job (ie with the consent of the organisation). It also does not apply where the individual acted in the reasonable belief they had in law the right to disclose. Any claim that an organisation has breached the Human Rights Act 1998 would be made against the organisation concerned. That should also be the case if someone were to seek compensation for the disclosure of their confidential information if this turned out to be wrong.

1.13 A significant volume of general information on data protection issues and specifically on data sharing, including processes by which personal data can be collected (eg through police-led Casualty Bureau) is already available (see Chapter 5 of this guidance for further information and references) and should be read by local and regional responders in conjunction with this publication.

Key Principles

- Data protection legislation does not prohibit the collection and sharing of personal data – it provides a framework where personal data can be used with confidence that individuals' privacy rights are respected.
- Emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do not share information.
- Emergency responders should balance the potential damage to the individual (and where appropriate the public interest of keeping the information confidential) against the public interest in sharing the information.
- In emergencies, the public interest consideration will generally be more significant than during day-to-day business.
- Always check whether the objective can still be achieved by passing less personal data.
- Category 1 and 2 responders should be robust in asserting their power to share personal data lawfully in emergency planning, response and recovery situations.
- The consent of the data subject is not always a necessary pre-condition to lawful data sharing.
- You should seek advice where you are in doubt – though prepare on the basis that you will need to make a decision without formal advice during an emergency.

Chapter 2
The Data Protection Act 1998

Summary

- The Data Protection Act 1998 provides a framework to strike a balance between the rights of individuals and other competing interests (paragraphs 2.1 and 2.6).
- There are various 'legitimising criteria' under the Act for sharing personal data (paragraphs 2.2–2.4).
- The criteria for data sharing are stricter for more sensitive personal data (paragraph 2.4).
- Myths surrounding what is required by the Data Protection Act 1998 have created unnecessary, and at times harmful, barriers to legitimate data sharing (paragraphs 2.6–2.15 and 2.20–2.22).
- Other issues relating to public interest, fair processing and disproportionate effort (paragraphs 2.16–2.19).

What the Data Protection Act means

2.1 The Data Protection Act was enacted in 1998 and applies in England, Wales, Scotland and Northern Ireland. It provides a framework under which personal data can be 'processed' providing it is lawful to do so. The Data Protection Act 1998 does not apply to any information which falls outside that defined as 'personal data'. The Data Protection Act 1998 aims to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal data. The way in which emergency planners and responders may use the personal data that they hold is governed by the **eight Data Protection Principles**.[7] These require that information is:

- processed fairly and lawfully and in accordance with a legitimising condition (see paragraph 2.2);
- processed for specified and not incompatible purposes;
- adequate, relevant and not excessive;
- accurate and up-to-date;
- not kept longer than necessary;
- processed in accordance with individuals' rights;
- kept secure; and
- not transferred to countries outside the European Economic Area without adequate protection.[8]

2.2 To comply with the principles of data protection as outlined above, data controllers[9] must:

- ensure that there is a legal basis for processing the data;
- ensure that the processing of the data is fair by giving data subjects the necessary information when personal data is collected, or if this is not possible that they are exempt from this condition (see paragraph 2.19);
- meet one of six conditions in order to process personal data as set out in Schedule 2 of the Data Protection Act 1998;[10]
- (if sensitive personal data is to be processed) meet one of a number of further conditions set out in Schedule 3 of the Data Protection Act 1998 and regulations authorised under that schedule (see paragraph 2.4 below);[11] and
- ensure that personal data is processed in accordance with the remaining principles of data protection as outlined above.

---

7 The Data Protection Act 1998 applies to anything at all done to personal data ('processing'), including collection, use, disclosure, destruction and merely holding personal data.

8 While this 'eighth principle' of the Data Protection Act 1998 is unlikely to be relevant to domestic emergencies, it may be relevant in international emergencies such as the Asian Tsunami. For further specific advice on applying this principle, see: **http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_eighth_data_prtection_principle_and_transborder_dataflows.pdf**

9 A *'data controller'* is a person who determines the purposes for which, and manner in which, personal data is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

10 See Schedules 2 and 3 of the Data Protection Act 1998 available at: **www.dca.gov.uk/ccpd/dpsubleg.htm**

11 Sensitive personal data is data relating to a person's ethnic origins, political opinions, religious beliefs, trade union membership, health, sexual life and criminal history.

2.3 As set out above, one or more Schedule 2 conditions should be met when disclosing personal information. **Data controllers need only comply with one condition** – they do not become 'more' lawful by being able to meet more than one condition. In addition, the conditions are just as important as one another – just because the 'consent' condition is listed first does not mean that it is more important than any other condition. The Schedule 2 conditions are broadly that:

- the subject has given consent to share information; or
- sharing information is necessary to protect the person's vital interests;[12] or
- sharing information is necessary to comply with a court order; or
- sharing information is necessary to fulfil a legal duty; or
- sharing information is necessary to perform a statutory function; or
- sharing information is necessary to perform a public function in the public interest; or
- sharing information is necessary for the legitimate interests of the data controller, or of the third party or parties to whom the data is disclosed, unless the rights or interests of the data subject preclude sharing.

2.4 As highlighted in paragraph 2.2, when information is sensitive then one or more Schedule 3 conditions must also be met.[13] These include that:

- the individual has given 'explicit consent' to share information; or
- sharing information is necessary to establish, exercise or defend legal rights; or
- sharing information is necessary for the purpose of, or in connection with any legal proceedings; or
- sharing information is necessary to protect someone's vital interests and the person to whom the information relates cannot consent, is unreasonably withholding consent, or consent cannot reasonably be obtained;[14] or
- sharing information is necessary to perform a statutory function; or
- is in the substantial public interest and necessary to prevent or detect a crime and consent would prejudice that purpose;[15] or
- processing is necessary for medical purposes and is undertaken by a health professional; or
- processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

---

12 Vital interests do not mean just 'life or death' situations but can also include situations where there is a risk of significant harm to life.

13 As for Schedule 2 conditions, data controllers only need to comply with one Schedule 3 condition, and no one condition is more important than another.

14 See paragraph 2.6. This condition likely to be particularly relevant in emergencies.

15 Under Schedule 3, the 'substantial public interest test' is tied to various other conditions which are set out in the Sensitive Personal Data Order 2000. The key condition of relevance to emergency planners and responders is that relating to law enforcement activities. By itself, 'substantial public interest' is not sufficient to meet the Schedule 3 condition unless it is associated with a law enforcement function.

2.5 The requirements of the Data Protection Act 1998 do not apply to data about deceased persons, including fatalities arising from an emergency, or any information from which an individual cannot be identified. Local and regional responders must though, of course, still be aware of, and take appropriate action to protect, the ethical, religious and cultural sensitivities of processing information relating to a deceased person.

What the Data Protection Act 1998 does not mean

2.6 The way in which the principles are interpreted and applied depends on the characteristics of each case. **Lessons from the 7 July 2005 response and other emergencies suggest that local responders may not be sufficiently aware of this flexibility.** Similar problems were identified in the Bichard Inquiry of 2004 which made recommendations on how to approach the provisions of the Data Protection Act 1998.[16] The following myths with their associated facts relating to the Data Protection Act 1998 should be considered by local and regional responders.[17] See **Annex A** for a flowchart illustrating the decision-making process for testing compliance with the Data Protection Act 1998.

Consent

2.7 Myth: You always need the consent of the data subject in order to share their personal data.

2.8 Fact: You do not necessarily need consent of the data subject to share their personal data.[18] In terms of compliance with the Data Protection Act 1998 (and the Human Rights Act 1998), consent of the data subject is not a necessary precondition for lawful data sharing. The Data Protection Act 1998 sets out a number of criteria under Schedule 2 for the legitimate processing of personal data (and sharing, like using, is for the most part just another form of processing) and if any one of the criteria is met, the Data Protection Act 1998 test is satisfied.[19] **Consent is simply one of the criteria.** Furthermore, consent in relation to personal data does not need to be explicit – it can be implied. More stringent rules apply to sensitive personal data, when consent does need to be explicit if that criteria is used – criteria other than consent can still be used for sensitive personal data.[20] Even without explicit consent for the sharing of sensitive personal data, it is still possible to share the data legitimately if this is necessary in order to exercise any statutory function (as may well be the case for responders) or to protect the vital interests of the individual where, for example, consent cannot be given.[21]

2.9 While sharing of personal data without the consent of the data subject may interfere with the right to respect for privacy under the Human Rights Act 1998 Article 8, the ECHR does allow for public authorities to interfere with certain rights under broadly defined circumstances known as 'legitimate aims'.[22] There must be a legal basis to share the information, the interference must be for the purpose of one of these legitimate aims and consideration must be given to whether the information sharing is proportionate and is the least intrusive method of achieving a legitimate aim.

---

16 See: **www.bichardinquiry.org.uk/**
Further guidance relating to this inquiry, specifically aimed at police forces, can be found at:
http://police.homeoffice.gov.uk/operational-policing/bichard-implementation/

17 Similar myths concerning the Data Protection Act 1998 have arisen in relation to other parts of society; see:
www.ico.gov.uk/upload/documents/library/data_protection/introductory/data_protection_myths_and_realities.pdf

18 You need to consider this issue in parallel with the common law duty of confidence – see paragraph 2.12 of this guidance.

19 'Processing' is a term used in the Data Protection Act 1998 and it includes obtaining, recording, holding and carrying out any operation on personal data.

20 See paragraphs 1.6 and 2.4 of this guidance.

21 This condition is likely to be particularly relevant in emergencies.

22 The legitimate aims in Article 8(2) of the ECHR are: the interests of national security, public safety or the economic well-being of the country; the prevention of disorder or crime; the protection of health or morals; or the protection of the rights and freedoms of others.

Compatibility

2.10 Myth: Personal data collected by one organisation cannot be disclosed to another organisation unless it is for the same (ie 'compatible') or a directly related purpose.

2.11 Fact: The issue of 'compatibility' arises under the second principle of the Data Protection Act 1998. If personal data is collected by one organisation for a particular purpose, then 'compatibility' (ie that the information must be used for the same purpose it was collected for) is not a necessary condition. The test is one of incompatibility – ie is the new purpose incompatible with the original purpose? In an emergency response scenario, **it is difficult to foresee circumstances where sharing personal data would be incompatible with the purposes for which they were originally collected.**

Confidentiality and Public Interest

2.12 Myth: The common law duty of confidence and/or the Human Rights Act 1998 prevents the sharing of personal data.

2.13 Fact: No, this is not the case. **Local responders need to balance the common law duty of confidence and the rights enshrined within the Human Rights Act 1998 against the effect on the individual or others of not sharing the information.** The common law duty of confidence relates to the duty for public bodies and individuals to respect confidential information relating to individuals. The information has to have a 'quality of confidence' – not everything that a public sector body holds on an individual will be confidential – and has to have been given in circumstances giving rise to an expectation of confidentiality.

2.14 If the data collection and sharing is to take place with the consent (either implied or explicit) of the data subjects involved, providing they are clearly informed about the purposes of the sharing, there will be no breach of confidentiality or the Human Rights Act 1998. If the information is confidential, and consent of the data subject is not gained, then the responder needs to satisfy themselves that there are grounds to override the duty of confidentiality in these circumstances. This can be because it is overwhelmingly in the data subjects' interests for this information to be disclosed. It is also possible that an overriding public interest would justify disclosure of the data (or that sharing is required by a court order or other legal obligation). To overcome the common law duty of confidence, the public interest threshold is not necessarily difficult to meet – particularly in emergency situations.

2.15 As indicated elsewhere within this guidance (see paragraphs 3.16, 4.3 and 4.5), confidential health data carries a higher threshold but it should still be possible to proceed where the circumstances are serious enough. As is the case for all personal data processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared – does all the personal data need to be shared to achieve the objective?

Other Aspects – the public interest

2.16 There is not a 'public interest test' as such set out in the Data Protection Act 1998 in relation to the processing of personal data. Providing the transfer of information is lawful, the fairness provisions are met and at least one Schedule 2 (and where necessary one Schedule 3) condition applies the transfer will be permitted.[23] In relation to the application of some of the conditions permitting processing there is a public interest consideration but this is not a formal test. Whether the disclosure is in the public interest is a useful question to ask when considering whether to share information. It can help to answer the fairness question if there is any doubt about it and it will be particularly relevant in considering whether to share confidential information.

[23] See paragraphs 2.2–2.3 of this guidance.

2.17 If the information is held under a separate duty of confidentiality, information may still be shared in the public interest. **Public interest may include the interests of the community as a whole, or groups within the community and of individuals.** In considering the public interest it is important also to consider the rights and general interests of the individual concerned and the likely harm both to them and to others if the information is shared or not shared. As is the case for sharing personal data about children to prevent or detect a serious crime, it may be **entirely proportionate for local and regional responders to share personal data to save life or prevent the possibility of serious harm** (for example, prior to potential flooding, or to offer post-event health screening to those caught up in terrorist attacks).

2.18 There may be **public interests which weigh against sharing the information**; for example the public interest in maintaining public confidence in the confidentiality of certain services. It is not possible to give guidance to cover every circumstance in which sharing of personal data without consent will be justified. Emergency planners and responders must make a judgement on the facts of the individual case. In making the decision they must weigh up what might happen if the information is shared against what might happen if it is not, and make a decision based on a reasonable judgement. Inevitably, this judgement will be on a case-by-case basis dependant on the nature of the emergency and the information in question, but the case studies provided in **Annex B** should help inform decisions.

Disproportionate effort

2.19 For personal data to be fairly collected, data subjects should be informed of any potential disclosures of their personal data and the potential uses of this when information is obtained directly from them. This is described as **'fair processing'** and the details can be stated in relatively broad terms and need not be in writing.[24] People can be told at the time their data is first collected or when it is shared (the former is preferable). When obtaining information from a third party, the data subject should again ideally be informed of the use of their data, unless they have already been informed by the third party when the data was collected, or when it would entail disproportionate effort. The disproportionate effort exemption (which is included in the Data Protection Act 1998) cannot be used when obtaining information direct from the data subject. It is advisable for organisations which are Category 1 and 2 responders to include in their 'fair processing notices' or 'subject information statements' that information may be shared in the event of an emergency situation in which they are involved.

Box 2.1: Experience from the 7 July 2005 attacks

When the initial Family Assistance Centre (FAC) was closing down, and the successor 7 July Assistance Centre was being set up, a Category 1 responder assessed that the contact details collected at the initial Centre could not legally be passed on to its successor organisation for ongoing, follow-up support. A similar situation arose with a charity telephone help line, where the information from the large number of individuals that had contacted the telephone help line was not passed onto the Assistance Centre because of legal concerns. The assumption of many families and survivors, however, was that the organisations would use the same database. They were therefore confused and irritated to find that they had been taken off contact lists or were asked to re-supply their details. Given that the role of the successor assistance centre was not incompatible with the original FAC, and that the successor centre had appropriate information management systems in place, the personal data should have been passed on. Further details on Humanitarian Assistance Centres and how they manage information flows can be found at: **www.ukresilience.info/.**

[24] Simply stating that the information may be passed to other government agencies and their partners for use in an emergency response or recovery context is sufficient.

Private sector

2.20 The Data Protection Act 1998 applies to all organisations – including private sector organisations or individuals – which hold or use personal data. A further **myth** about the Data Protection Act 1998 is that the private sector cannot be forced to release personal data. The **facts** are less clear cut. Generally the private sector cannot be forced to release personal data. The Data Protection Act 1998 does not, either, enable emergency responders to force the private sector to disclose information. However, it is possible to obtain an order of the court for the private sector to disclose information (including personal data) if this is necessary for a particular purpose and there is a legal basis. The police also have separate powers to compel organisations, including those in the private sector, to provide information for law enforcement purposes.

2.21 This means that the Data Protection Act 1998 allows for the disclosure of personal information from a private company to the police where the latter need the information for their law enforcement functions (which includes preventing or detecting crime and apprehending and prosecuting offenders). Aside from this and court orders, the Data Protection Act 1998 has exemptions that would *allow* private sector organisations to share data in particular situations, but it cannot *compel* them to.

2.22 Parts of the private sector have a fairly mechanistic (and hence slow) approach to considering the release of confidential (ie customer) data. This is particularly true of the financial and telecommunications sectors where regulations above and beyond the Data Protection Act 1998 impose strict rules on customer confidentiality. Category 1 and 2 responders should be aware that they have limited powers to compel private sector organisations (beyond those that are Category 2 responders – see paragraph 3.3) to share personal data. Emergency responders should instead establish good contacts with private sector organisations to ensure data sharing happens as quickly as possible when required.

Chapter 3
The Civil Contingencies Act 2004

Summary

- Clear legal power to share data is found in secondary legislation made under the Civil Contingencies Act 2004 (paragraphs 3.1–3.3).
- Information sharing agreements can be useful but are not a necessary requirement (paragraph 3.10).
- Potential use of geographical information systems (paragraphs 3.11–3.12).
- Importance of exercising and training (paragraphs 3.13–3.14).
- Internal policies should be consistent with legal requirements (paragraphs 3.15–3.16).

The Civil Contingencies Act 2004

3.1 The Civil Contingencies Act 2004 provides a **framework for modern civil protection efforts** by establishing a clear set of roles and responsibilities for local responders, giving greater structure and consistency to local civil protection activity, and establishing a sound basis for performance assessment at a local level.[25]

3.2 Though the key law governing data protection is the Data Protection Act 1998, **clear legal power to share data is found in secondary legislation** made under the Civil Contingencies Act 2004. The Civil Contingencies Act 2004 (through the regulations made under it) places a duty on Category 1 and 2 responders, on request, to share information relating to emergency preparedness/civil protection work with other Category 1 and 2 responders. This duty relates to the preparedness, response and recovery stages of an emergency.[26]

3.3 Section 2.4 of the statutory guidance supporting the Act states that:

"Information sharing is necessary so that Category 1 and 2 responders are able to make the right judgements. If Category 1 and 2 responders have access to all the information they need, they can make the right decisions about how to plan and what to plan for. If they do not have access to all information, their planning will be weakened."

This information sharing duty is not a statutory obligation to breach the common law duty of confidentiality – where the information is confidential the party considering making the disclosure must consider whether the interests of the individual or individuals will be better served by making the disclosure (ie is it in the public interest – see paragraph 2.16).[27] But it does provide one of the legitimising criteria (see Chapter 2, paragraphs 2.1–2.4) for the sharing of personal data under the Data Protection Act 1998 (and if no duty of confidence is breached should put beyond doubt it is lawful under the first Data Protection Principle – see paragraph 2.1). Necessary actions taken under the Civil Contingencies Act 2004 in accordance with the data sharing requirements of the Contingency Planning Regulations[28] will be compliant with the Data Protection Act 1998 if:

- a legitimising condition is met (or in relation to sensitive personal data, one condition from Schedule 2 and one condition from Schedule 3 of the Data Protection Act 1998 are met);
- information is being shared for a specific purpose;
- information is being shared for a limited time;
- information is only to be shared between named Category 1 and 2 responders that have a defined (as assessed by the requesting organisation or individual) need to see it; and
- the data subjects are informed that their data may be shared within government for emergency response or recovery purposes unless to do so involves disproportionate effort.

---

[25] Guidance on Part 1 of the Civil Contingencies Act 2004 is available at: **www.ukresilience.info/ccact/index.shtm**

[26] *Emergency Preparedness,* Chapter 3. The full details are provided in regulations 45 to 54 of the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 and regulations 39 to 47 of the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005.

[27] This means it is not a 'mandatory gateway' that imposes an absolute legal obligation on public bodies to provide relevant information to one another. Rather the party should confirm that a legitimising condition of the Data Protection Act 1998 is met, and that there would not be a breach of the common law duty of confidence in sharing the data.

[28] Regulations 45 to 54 of the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 state that should a Category 1 or 2 responder reasonably require information held by another Category 1 or 2 responder in connection with the performance of their duties or functions relating to emergencies, then such information (including personal data) may be requested and that the responder receiving the request must comply unless an exemption applies.

3.4 The Civil Contingencies Act 2004 does also prohibit Category 1 and 2 responders from publishing or otherwise disclosing any 'sensitive'[29] information which they have received by virtue of the Civil Contingencies Act 2004 or created in the course of discharging their duties under the Act.[30] Confusion has arisen over the use of the word 'sensitive' in both the Civil Contingencies and Data Protection Acts. The Acts have different definitions of what constitutes 'sensitive'. Under the Civil Contingencies Act 2004, sensitive information relates to **national security, public safety, business or personal data**. Only the latter is covered by the use of 'sensitive' in the Data Protection Act 1998. Under the Civil Contingencies Act 2004, the only two exceptions where sensitive information can be disclosed are when:

- consent for the publication or disclosure is obtained; or
- the information is commercially sensitive or personal data, but the public interest in disclosure outweighs the interests of the person or organisation concerned.[31]

3.5 Category 1 and 2 responders should be aware of the differences required in handling personal data (as outlined in this document) when compared to handling sensitive security-related or commercial information.

Devolved administrations

3.6 The way in which the information sharing duty under the Civil Contingencies Act 2004 applies to Category 1 and 2 responders in Scotland, Wales and Northern Ireland is in much the same as in England. The key points in relation to the information sharing duty, which are provided in more detail in the statutory *Emergency Preparedness* guidance, are:[32]

- in Scotland, Part 1 of the Civil Contingencies Act 2004 (which includes the disclosure of information provision under which the Regulations were made) applies to Scotland, with the powers it sets out residing with Scottish Ministers;
- in Wales, arrangements under Part 1 of the Civil Contingencies Act 2004 apply; and
- in Northern Ireland, duties in the Civil Contingencies Act 2004 apply only to a limited number of organisations which deliver functions which are not transferred (namely the Police Service of Northern Ireland, the Maritime and Coastguard Agency and telecommunications operators).

---

29 The variety of types of 'sensitive information' and in some circumstances, the person or organisation whose consent is needed, are defined in Regulations 45 and 51 of the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 and provided in *Emergency Preparedness*, Chapter 3. The definition of sensitive personal data under the Data Protection Act 1998 is provided in Chapter 1 of this guidance.

30 *Emergency Preparedness,* Chapter 3.

31 The detailed rules on disclosure are found in Regulation 51 of the 2005 Regulations (Regulation 45 of the Scottish Regulations). The consent exception does not apply in relation to sensitive information adversely affecting national security if a Minister has issued a certificate to that effect. This public interest exception does not apply if the information is sensitive by virtue of its national security or public safety implications. In addition, where it does apply the responder needs to notify the person concerned.

32 See *Emergency Preparedness*, Chapters 10, 11 and 12 on Scotland, Wales and Northern Ireland respectively.

Data Collection

3.7 The collection of personal data prior to or during an emergency is a key part of emergency planning, preparation and response. Emergency planners and responders may need to maintain lists of all those people who could be affected by an emergency. As long as such a list is kept securely, with access only to those who need to see the information (in compliance with the requirements of the Data Protection Act 1998 outlined in Chapter 2 of this guidance) and it is not used for any other purpose – then the collection will be permitted. It is important that the purposes for the collection of this personal data are in the interests of the data subject and more generally the public at large.[33] The organisation that kept such a list would become the data controller with attendant responsibilities, including providing subject access rights. In addition if the data is to be obtained from other data controllers these controllers must ensure that the data subjects are aware of the disclosures.[34] The maintenance of such lists or databases (which could be linked to Geographical Information Systems – see paragraph 3.11) can allow the data to be checked (ie quality assured) prior to an emergency – an important step to provide emergency responders confidence in decisions based upon the data. A key issue in meeting the requirements of the Data Protection Act 1998 will be maintaining the accuracy of the data – it is likely to need regular checking and sharing with those who provided it.

3.8 As an alternative to maintaining their own lists or databases of personal data to inform a response to an emergency, local and regional responders can put in place mechanisms by which they can draw upon individual organisations detailed records during an emergency (such as those of care homes, voluntary organisations and health trusts). There are possible advantages and disadvantages to such an approach. On the negative side, they could be less responsive than the use of pre-existing aggregated lists or databases because of the bureaucratic/practical hurdles in accessing them. On the positive side, they should be more accurate given that they will be using the latest version of the organisation's records (eg a care home's residents list). In either case, well developed and tested arrangements should be in place to ensure that records are accessible and accurate, and that 'fair processing' procedures are in place to inform individuals that information about them is included in such a list or database.[35]

3.9 The processing of personal data by local and regional responders must be proportionate to the requirements. Emergency planners and responders should only process personal data that they really need. As an example, during the planning stage it might be important to know the total numbers of vulnerable people in an area to ensure that adequate facilities and procedures exist. In these circumstances it should be legitimate for the planning agency to request the numbers and locations of vulnerable people, but not additional personal data which would allow identification.[36]

---

[33] See paragraph 2.12 of this guidance.

[34] For more information on subject access rights see: **www.dca.gov.uk/ccpd/faqdp.htm**

[35] See paragraph 2.19 of this guidance.

[36] It should be noted, however, that in the hands of the giver, the sharing of addresses of vulnerable people without names is still personal data, with the accompanying Data Protection Act 1998 obligations – it is just the concerns about privacy are not nearly as high.

3.10 It is important that the organisations involved in emergency planning establish processes to manage the disclosure or exchange of personal data effectively so that the parties involved are quite clear about both the type of information that could be shared and the circumstances providing for disclosure. The local authority, through the Local Resilience Forum (LRF) structure, is generally in the best position to lead on the establishment of multi-agency data sharing agreements. DCA has developed a toolkit for the public sector to enable effective and legitimate personal data sharing.[37] For organisations that engage in large volume transfers of personal data (for example, in parts of the social security and health systems), detailed data sharing protocols may be appropriate. In general, however, more strategic agreements (or Memorandums of Understanding) setting out the high level arrangements and principles underpinning data sharing will be more appropriate. These provide a flexible data sharing framework for multi-agency emergency management which more detailed mechanistic information sharing agreements may not. **The absence of data sharing agreements should not prevent Category 1 or 2 responders from sharing data particularly when responding to an actual emergency event**.

GIS and Data Sharing

3.11 Geographical Information Systems (GIS) are frequently used to facilitate the sharing of geographically-referenced data and information. Given that in excess of 90% of corporate data is estimated to be geographically referenced in one form or another (for example, associated with an address, a postcode or a grid reference) the application of GIS to emergency management is growing in significance, and the Emergency Planning College has published guidance on GIS and promoting its uptake.[38] Inappropriate barriers to sharing data between agencies have, however, impeded a number of GIS initiatives. One example was the refusal of one agency, incorrectly citing the Data Protection Act 1998, to provide the locations and basic details of poultry farms to assist in avian flu risk assessment and emergency planning.

3.12 Many of the data-sets which GIS can utilise to support effective and efficient emergency preparation, response and recovery fall well outside the focus of data protection legislation, for example area demographic profiles, flood risk zones, hazardous sites and infrastructure networks. Full or partial release of data relating to some of these may of course be subject to other constraints around national security, public safety and commercial confidentiality.

Exercising and training

3.13 Exercising and training is a key element of risk-based planning. Category 1 responders have a duty to maintain and exercise their plans under the Civil Contingencies Act 2004. Category 2 responders are obliged to co-operate in this. The regulations also require provisions for the training of staff and other persons to be included in plans.[39]

3.14 Exercising of information management components of plans and table-top or discussion based exercises can be used to test data sharing processes. Exercises could and may include personal data sharing scenarios so that organisations and individuals can develop their understanding of the types of decisions they may need to make in an emergency. The case studies at **Annex B** provide some ideas for possible scenarios to include in wider exercise play. Training should similarly include data sharing as part of any wider information management training. Given their critical role in emergency management, the training of incident commanders and any identified information co-ordinators/managers in managing personal data appropriately is particularly important.

---

[37] See the DCA's website: **www.dca.gov.uk** for examples of information sharing protocols and agreements

[38] *A Guide to GIS Applications in Integrated Emergency Management* is available at: **www.ukresilience.info/publications/gis-guide_acro6.pdf**

[39] *Emergency Preparedness,* Chapter 5.

Internal processes

3.15 In making any decision to share information or not, the organisation should always record the reasons for the decision. If the decision is to share data, then the organisation should record what the information was and who it was shared with. This process should form part of the organisation's wider information management processes.

Box 3.1: Internal policy challenges

During the emergency response to the 7 July 2005 attacks, a Category 2 responder affected by the attack requested information from a Category 1 responder. The responder consulted with their information co-ordinator and legal advisors who advised that the personal data could be transferred. Even with this advice, however, the internal policy of the Category 1 responder meant that the personal data was not disclosed.

In this case, the Category 1 responder's policies were inconsistent with the Data Protection Act 1998 and actually presented a higher barrier to share the information than was legally necessary.

3.16 As the text box above illustrates, some data sharing problems have arisen because organisations' internal policies are inconsistent with legal requirements. This may be because of:

- misunderstanding of the legal framework of the Data Protection Act 1998 – which this guidance should help to rectify;
- legal guidance on the Data Protection Act 1998 has evolved since its original development. The regulator (the Information Commissioner) takes a purposive and common sense approach to such elements as 'compatibility' and 'lawfulness'.[40] It is important, therefore, for local responders to review regularly their internal information sharing guidance to ensure it is consistent with the official legal guidance; and
- a culture of risk averseness among senior decision-makers or information managers in the emergency community surrounding data protection issues. This guidance combined with further multi-agency training and exercising should help to shift this culture towards one of effective risk management.

[40] See Chapter 2 of this guidance.

Chapter 4
Other legislation

Summary

- Other legislation relevant to data sharing issues include:
  - Human Rights Act 1998 (paragraphs 4.1–4.2).
  - The Freedom of Information Act 2000, the Environmental Information Regulations 2004, the Local Government Act 2000, the Crime and Disorder Act 1998, the Police Act 2006 and the Children Act 2004 (paragraph 4.3).
  - Various health-related legislation, including the Access to Health Records Act 1990, the Access to Medical Reports Act 1988, the Health and Social Care Act 2001 and the Public Health (Control of Diseases) Act 1984 (paragraphs 4.3–4.5).
- Devolved administrations should take account of their own legislation as not all of the above laws are UK-wide.

Other legislation

4.1 There are a variety of other pieces of legislation that relate to the collection and sharing of personal data that may be relevant to emergency planners and responders. Some of this legislation will not apply directly to the devolved administrations and different jurisdictions should take account of their own legislative arrangements. The most significant is the Human Rights Act 1998 which applies throughout the UK and which provides people with a clear legal statement of their basic rights and fundamental freedoms. Article 8 of the ECHR was incorporated into UK law by the Human Rights Act 1998. It relates to the right to respect for private and family life, home and correspondence. If the data collection and sharing is to take place without the consent of the data subjects involved, or if bulk transfers are being made which do not specifically relate to individuals who are involved in an emergency situation, then Article 8 is relevant.

4.2 The Human Rights Act 1998 does not, though, prevent the collection or sharing of personal data. The Human Rights Act 1998 provides lawful restrictions on these human rights for use by public authorities in certain circumstances such as reasons of national security, public safety, the protection of health and the prevention of disorder. Public authorities can, therefore, collect and share personal data if it is in pursuit of these lawful aims – of which sharing of personal data in an emergency is likely to be legitimate.

4.3 Other relevant pieces of legislation include the:

- **Freedom of Information (FOI) Act 2000** deals with access to information (excluding environmental information) held by public authorities by any person, but specifically excludes access to personal data.
- **Environmental Information Regulations 2004** which deals with access to environmental information held by public authorities.
- **Local Government Act 2000** which gives local authorities powers to take any steps which they consider are likely to promote the well being of their area or the inhabitants of it. Section 3 of the Act is clear that local authorities are unable to do anything – including sharing information – for the purposes of the well being of people where they are restricted or prevented from doing so by other legislation (eg Human Rights Act 1998 and Data Protection Act 1998) or by the common law duty of confidentiality.
- **Crime and Disorder Act 1998** which sets out in Section 115 the power of any organisation to share information with the police, local authorities, Probation Service and health authority (or anyone acting on their behalf) for the purposes of the Act (which basically relate to the prevention, detection and reduction of crime and disorder). The police have a general common law power to share information to prevent, detect and reduce crime.
- **Police Acts 2006 and 1997** which permit the Secretary of State to issue codes of practice relating to the discharge by police authorities of any of their functions. A code of practice has been issued which sets out the principles governing the management of information (including personal information).[41]
- **Children Act 2004** which places a duty on agencies involved in children's welfare provision to safeguard and promote children's welfare. This has implications for data sharing given the sharing of information on children is required to ensure that they get the services and support they require, and to protect them from abuse or neglect.[42]
- **Access to Health Records Act 1990** which has mostly been superseded by the Data Protection Act 1998, and now primarily governs access to the health records of deceased people.

---

41 See: http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/Bichard_-_MoPI_Guidance_INT2.pdf

42 See Department for Education and Skills (DfES): www.everychildmatters.gov.uk/_files/80F6F91212565EDE7446110B89A43817.pdf

- **Access to Medical Reports Act 1988** which governs access to medical reports produced about patients, by the clinician normally concerned with their care, for employment and insurance purposes.
- **Health and Social Care Act 2001** which provides powers for the Secretary of State (for Health) to permit the use of prescribed patient information for medical purposes in the interests of improving patient care or in the public interest where it is impracticable to obtain informed consent from the patients concerned.[43] While these powers are relevant to data sharing, the processes set out under the Health and Social Care Act (Section 60) are unlikely to be applicable in the short time scales of emergency response. They may be relevant, however, for strategic planning purposes and in the recovery stage (eg the HPA used the Health and Social Care Act to collect personal data from Accident and Emergency (A&E) department notes following the 7 July 2005 attacks to inform the longer-term public health response).
- **Public Health (Control of Diseases) Act 1984** which includes provisions for use by local authorities to control and prevent the spread of infectious disease. This includes giving local authorities the power to require occupiers of premises where a case of a specified disease has occurred to provide information for the purpose of enabling measures to be taken to prevent the spread of the disease or to trace the source of any food poisoning. This information is likely to include the names and addresses of the users and occupants of the premises.

4.4 While local responders clearly need to have due regard to these other pieces of legislation, the key framework for data protection and sharing is that provided by the common law of confidence and the Data Protection Act 1998. Among the various types of personal data that local responders may need to obtain or share is medical information which is subject to greater legislative and regulatory safeguards when compared to most forms of other 'personal data'. Specific guidance can be referenced in the legislation cited above, but in most circumstances the key issue will remain that of balancing the duty of confidence against public interest needs.

Medical and health code of practice

4.5 The NHS Code of Practice on Confidentiality provides advice and guidance on the legal, ethical and policy conditions affecting the disclosure of **confidential patient information**.[44] In simple terms, in the absence of a patient's consent, information should only be disclosed where there is a statutory obligation to do so or where the public interest in disclosure is sufficient to override both the duty of confidence owed to an individual and also the public interest in keeping health records confidential. The threshold for disclosure will be a relatively high one.[45]

[43] See the Health and Social Care Act 2001, Section 60 at: www.opsi.gov.uk/acts/acts2001/10015--g.htm

[44] See: http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsArticle/fs/en?CONTENT_ID=4100550&chk=1w6ljh

[45] See the Department for Health's website for more information on patient confidentiality: http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/fs/en

Chapter 5
Further information and references[46]

Emergency Preparedness
www.ukresilience.info/ccact/eppdfs/index.shtm

Emergency Response and Recovery
www.ukresilience.info/ccact/errpdfs/index.shtm

Bichard Inquiry
http://police.homeoffice.gov.uk/operational-policing/bichard-implementation/

Management of Police Information
http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/Bichard_-_MoPI_Guidance_INT2.pdf

Management of children-related information
www.everychildmatters.gov.uk/resources-and-practice/IG00065/

Youth Justice Board and the ACPO Sharing Personal and Sensitive Personal Information on Children and Young People at Risk of Offending: A Practical Guide (2005)
http://www.yjb.gov.uk/Publications/Resources/Downloads/infosharing0305.pdf

Patient confidential information guidance
http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/fs/en

Confidentiality: NHS Code of Practice
http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsArticle/fs/en?CONTENT_ID=4100550&chk=1w6ljh

General Medical Council: Confidentiality: protecting and providing information
http://www.gmc-uk.org/guidance/current/library/confidentiality.asp

Health Protection Agency (HPA) 7 July 2005 Response publications and leaflets
www.hpa.org.uk/london_bombings/response.htm

Leeds NHS best practice publications
www.leeds.nhs.uk/infoshare/

Resilience Websites
www.ukresilience.info
www.preparingforemergencies.gov.uk

Department for Constitutional Affairs
www.dca.gov.uk
www.dca.gov.uk/foi/sharing/toolkit/index.htm

Information Commissioner's Office
www.ico.gov.uk

Information sharing vision
www.dca.gov.uk/foi/sharing/information-sharing.pdf

Reaching Out: An Action Plan on Social Exclusion
www.cabinetoffice.gov.uk/social_exclusion_task_force/reaching_out

Home Office
www.homeoffice.gov.uk

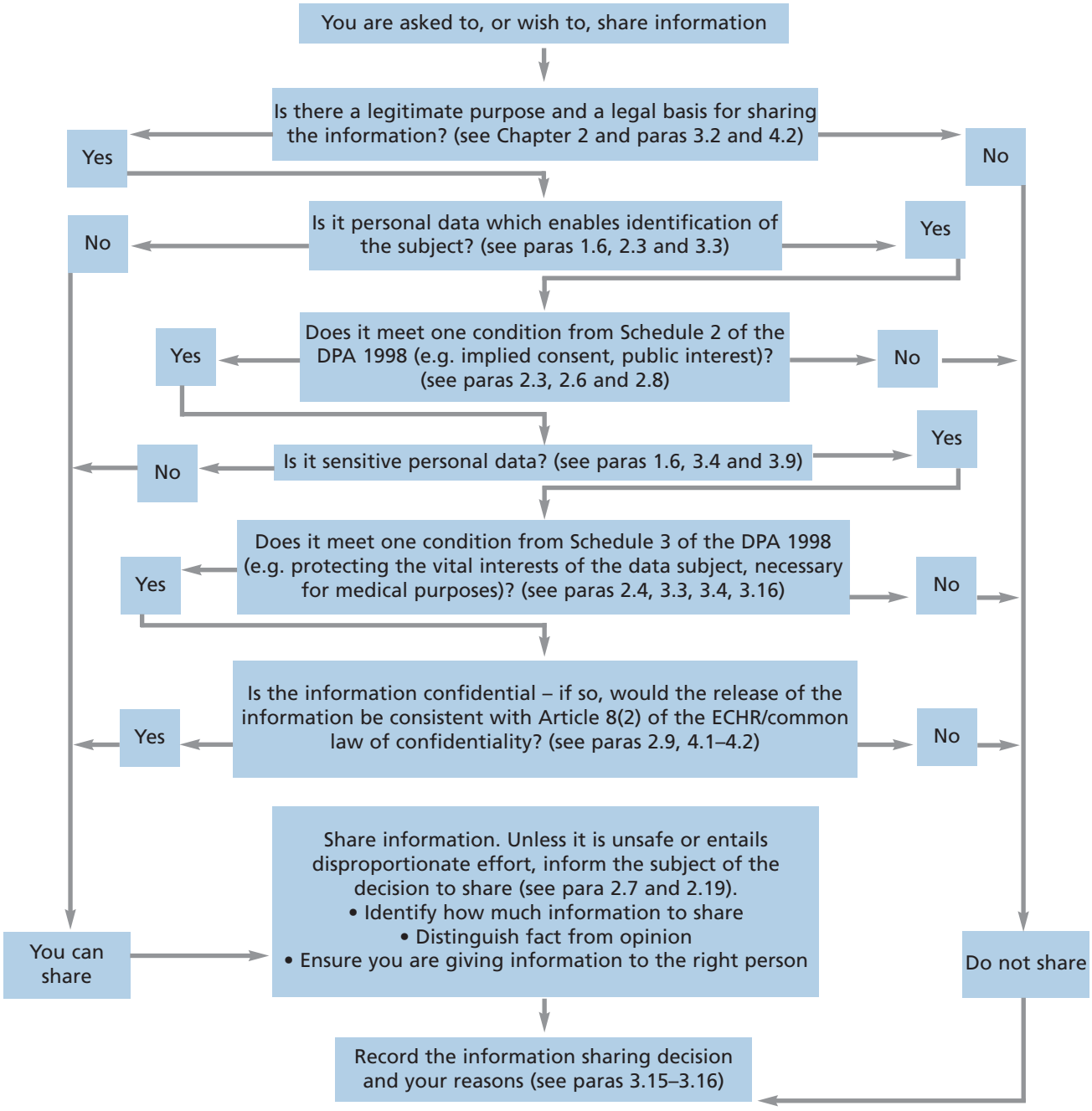
[46] All websites and links accessible as at December 2006.

Department of Health
www.dh.gov.uk/

Health and Safety Executive
www.hse.gov.uk

Many of the resources mentioned in this document can be found at the Emergency Planning College Library and Information Centre
www.epcollege.gov.uk

Annex A
Flowchart of key principles for information sharing[47]



[47] Adapted from Information Sharing: A Practitioners Guide.

Annex B
Case Studies[48]

Case Study 1 Scenario: A terrorist attack in a major city has occurred. The police-led Casualty Bureau has compiled lists of people who have been, or are believed to have been, caught up in the incident. The local NHS trust wants the lists of individuals to use as a basis for follow-up health care work. The Casualty Bureau has not gained explicit consent from those individuals who have provided their personal data information. What should the Casualty Bureau do?

Outcome: There are a number of factors which the Casualty Bureau needs to take into account. The first step will be to ensure that there is a legal basis for the transfer. As the information will be held by a Category 1 responder and the information is reasonably required by the NHS Trust in connection with the performance of a function which relates to an emergency, the legal basis will be under the Civil Contingency 2004 (Contingency Planning) Regulations 2005. The Casualty Bureau then needs to consider the nature of the information. If the information is about the individuals' state of health, then it will be sensitive personal data under the Data Protection Act 1998 and consent cannot be implied. However, it is possible to consider other conditions, such as that concerning the 'vital interests' of the data subject. This does not just mean life or death situations but can also include situations where there is a risk of significant harm to life, in which cases it is also likely that the 'legitimate interests' condition will apply. If the data is sensitive then a condition permitting the processing of sensitive data is also required. Schedule 3 of the Data Protection Act 1998 provides the conditions for the fair processing of sensitive data. At least one condition needs to be met. Where the 'vital interests' condition is used (and in the absence of another condition being met, such as explicit consent), then vital interest only applies where: consent cannot be given; and/or consent cannot be reasonably obtained; and/or in cases of the vital interests of another person consent has been unreasonably withheld by or on behalf of the data subject. In this case (ie sensitive data without explicit consent), then it is likely to be reasonable to expect the Casualty Bureau to contact the patients and ask them to contact their local NHS trust, and to ask them for their consent for their personal data to be shared.

If the data is not clearly sensitive, then it will be possible to rely on another legitimate condition under Schedule 2 of the Data Protection Act 1998, such as '*for the exercise of any other functions of a public nature exercised in the public interest by any person*'. To ensure Data Protection Act 1998 compliance it will also be necessary to inform the individuals concerned that their information is being passed to the NHS, explaining why – this need not, though, necessarily happen prior to the information sharing.

[48] Other case studies, though not directly related to the emergency context, are available from the DCA and DfES websites. See: **www.dca.gov.uk/foi/sharing/toolkit/casestudies.htm** and **www.everychildmatters.gov.uk/_files/80F6F91212565EDE7446110B89A43817.pdf**

Case Study 2 Scenario: A major industrial accident has occurred. The local authority leads in the establishment of a Humanitarian Assistance Centre to provide a one-stop-shop for support to those affected by the incident, and their family and friends. The Humanitarian Assistance Centre is being encouraged by the local media to release all the personal details of those caught up in the disaster. What should the Assistance Centre do?

Outcome: The Humanitarian Assistance Centre needs to consider if it has the legal power to make the disclosure. Like Local and Regional Resilience Forums who are not statutory bodies or Category 1 or 2 responders, the Humanitarian Assistance Centre is not a Category 1 or 2 responders or a statutory body. The Centre does not, therefore, have the power to make the disclosure under the Civil Contingencies Act 2004. That said, the organisations that make up the Humanitarian Assistance Centre will include Category 1 and 2 responders. The lead authority in the Humanitarian Assistance Centre, for example the local authority, should make the decision on whether to disclose the information (in consultation with other stakeholders). In making that decision, the local authority will need to weigh the possible public interest benefit of releasing the personal data to the media, against the possible detriment this may cause to the individuals, taking into consideration the common law duty of confidentiality and the requirements of the Human Rights Act 1998. If the data is sensitive, it would be difficult to find an appropriate Schedule 3 condition.

Given that there will be little public interest benefit from releasing the names to the media (rather it is likely to be the opposite given the individuals will be exposed to media intrusion), and that once the names are released they are no longer under any managed control by the Assistance Centre, then the Centre (or its constituent organisations) should not release the data.

Case Study 3 Scenario: An LRF sub-group for flooding is preparing plans for responding to a flood emergency. They want to pull together a list of all the people who are potentially vulnerable into one central database in order for it to be at hand in the event of a serious flood warning. Can they legally do this?

Outcome: There is likely to be a legal basis for a local responder within an LRF having a database of their own but this would mean they would become a data controller in their own right for this information with the associated responsibilities, which would include ensuring the data remained accurate and up to date.[49] Alternatively, local responders within the LRF can set up a data sharing agreement between themselves and the data controllers for the information they require. This information could then be drawn upon when an emergency situation arose. At that point the relevant lead authority within the LRF would become a data controller for the information.[50] In both cases, the 'fair processing' requirement under the Data Protection Act 1998 means that the data controller needs to inform the individuals that information about them is included in the database.[51] The easiest time to do this is generally at the point of collection of the data.

[49] Under the Data Protection Act 1998, 'data controller' means a person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons. An LRF is not a separate entity for the purpose of being a data controller – a responder within the LRF will need to be the data controller.

[50] See paragraphs 3.7–3.9 of this guidance.

[51] See paragraph 2.19 of this guidance.

Case Study 4 Scenario: A water company has applied to the Secretary of State for the Environment, Food and Rural Affairs (Defra) for an Emergency Drought Order to enable them to interrupt the public water supply on the grounds of anticipated problems arising from extreme drought conditions. The water company wants to identify those individuals whose health could be at risk should they not have immediate access to sufficient emergency supplies of water. They have requested that social services, the health authority and voluntary organisations furnish them with names and addresses of people residing in the area likely to be affected who fall into this category. Should the local authority, health authority and voluntary organisations release the information?

Outcome: For the purposes of this scenario, we will assume that consent has not been received and that it is impractical to get the data controllers to write to the data subjects in the time available.

The water company is a Category 2 responder and where reasonably required is entitled to ask the other responders – social services and health authority – to share the information under the Civil Contingencies Act 2004. Voluntary organisations may be able to share relevant information under general powers. As the information is specific and limited to a few individuals it is likely that this will be permitted by the Data Protection Act 1998.

The local authority, health authority and voluntary organisations need to balance their common law duty of care and the public interest served by providing the names and addresses, against those individual's right to confidentiality and privacy. In the first instance, though, the local authority and voluntary groups should test whether the water company really needs the names and addresses for their purposes – will the addresses just suffice (and hence not be subject to the same concerns about individuals' privacy)?[52]

Assuming for the purposes of this case study, that the names and addresses are required, the information can be provided under the legitimate interest provision. It is unlikely that sensitive personal data will be required as it will not be necessary to explain why the individuals need special considerations. The local authority should in addition seek confirmation from the water company that they will only use the personal data for mitigating the effects of water supply interruptions and not other incompatible purposes (for example direct marketing).

Case Study 5 Scenario: An emergency (either natural or man-made eg terrorist incident) occurs overseas with many British nationals involved. The police-led Casualty Bureau, on behalf of the FCO, has compiled lists of individuals who have been reported as having been, or are believed to have been, caught up in the incident. A reception centre is established at Heathrow for those returning to the UK and the police-led team has compiled lists of people returning on the flights. The following requests are made:

(i) The British Red Cross is asked by the Government to establish a virtual Assistance Centre for those involved and their families. DCMS and Red Cross ask the FCO (and through them, the police) for the names and contact details of those involved.

(ii) DCMS want to write to the survivors and bereaved families to reiterate information about sources of support etc and for the minister to send a letter of condolence.

(iii) DCMS are tasked with arranging a memorial service in the UK for those who died. They ask the FCO (and through them, the police) and the British Red Cross for the names and contact details of those involved.

(iv) The National Audit Office (NAO) contracts a well known organisation/agency (a trust) to conduct a survey of those who were involved, either as direct survivors, or as bereaved family members, to examine the Government's response to their needs. The Trust asks the NAO for the names and contact details. The NAO in turn asks the FCO, police, DCMS and voluntary organisations for the names and contact details.

[52] See paragraph 3.9 of this guidance.

Outcome: In all cases, the answer is yes, although the circumstances and methods employed are nuanced. In the first three cases, the only information shared should be the names and addresses (ie not additional information relating to the person's involvement in the emergency), with the sharing of it coming under Schedule 2 (because it is not sensitive personal data) of the Data Protection Act 1998. The sharing of this information meets the principles of the Data Protection Act 1998 if it is processed fairly and lawfully.

In terms of what constitutes 'fairly and lawfully', meeting a schedule 2 and/or 3 condition will not (on its own) guarantee that the processing is fair and lawful. This general requirement needs to be satisfied as well as the Schedule condition(s). The fairness requirement relates to whether the data subject has been misled or deceived, and that so far as is practicable they are informed of the use of their data (see paragraphs 2.7, 2.8 and 2.19 of this guidance). In these four cases, it is reasonable to assume the 'fairness' criteria have been met. If the collecting agency has informed the data subject of the potential use of their data (see paragraph 2.19) which they ideally should by including the task in their standard operating procedures, then informing the subject of the sharing of their information is unnecessary. If the collecting agency has not, then it is likely to entail disproportionate effort to do so at this point.

As for 'lawfulness', the sharing of the data is contributing to statutory functions of the police, DCMS and the FCO. In considering any duty of confidence, in the first three cases there are sound public interest reasons to share. In the fourth, the virtual Assistance Centre should contact the data subjects to check that they are content.

Given the fairness and lawfulness test is passed, the next step is to consider whether Schedule 2 conditions are met. In the first three cases a number of Schedule 2 conditions are met:

- it is acceptable to assume implied consent given the 'data subjects', when providing details to the Casualty Bureau, are likely to have assumed that the details would be used by other official bodies as well as non-government organisations such as the British Red Cross working on behalf of government; and
- though the virtual Assistance Centre and condolence letters are unlikely to fall under the 'vital interests' condition (condition 4 under Schedule 2 of the Data Protection Act 1998), they are part of the government's functions (ie humanitarian assistance in an emergency) and are undertaken in the public interest (ie to offer practical and psychological support) so it would meet condition (c) and/or (d), paragraph 5, of Schedule 2.[53]

A high level data sharing agreement between DCMS and the British Red Cross (or more generally, the Voluntary Sector Civil Protection Forum) may also help to facilitate the data sharing by providing additional assurance that the data is kept securely and only kept for so long as it is needed.

[53] Under Schedule 2, Paragraph 5 of the Data Protection Act 1998, condition (c) is *'for the exercise of any functions of the Crown, a Minister of the Crown or a government department'*. Condition (d) is *'for the exercise of any other functions of a public nature exercised in the public interest by any person'*.

In the case of the fourth request (from the NAO), it is not clear that 'implied consent' is present given that the personal data is being shared with an organisation, albeit an official organisation (ie the NAO), that is not directly involved in the emergency and is then passed on to a third party (ie the trust) outside of government. The virtual Assistance Centre should first, therefore, contact the data subjects to check that they are content for their information to be passed to third party for the sole purposes of the survey. If they are, the Assistance Centre would then, as data controller, need to assure itself that both third parties have the appropriate information management processes in place. One mechanism to ensure the personal data is kept appropriately and securely is to make all the information anonymous.[54]

Case Study 6 Scenario: A terrorist incident has occurred in a major UK city. Many individuals who were treated at the scene or who were uninjured left the incident site without giving their details to the police or any other local responders. Local responders now want to identify individuals who were exposed to the effects of the terrorist attacks in order to offer/provide appropriate health (including psychological) advice and support. What can they do?

Outcome: The local authority or the appropriate health organisation can request members of the public caught up in the terrorist incident to provide their contact and GP details, and the place and nature of their exposure to the incident. In collecting the personal data, the requesting organisation will need to be clear on the requirements and use of the information (ie it is part of the public health response to the incident) and the measures that will be taken to control the information appropriately.[55]

Case Study 7 Scenario: A train carrying industrial waste collides with a commuter train on the outskirts of a city. The local A&E departments treat many wounded passengers. The next day it is found that the industrial waste included dangerous materials that were released during the crash. The HPA requests lists of patients seen in the A&E departments so that it can follow-up those involved in order to advise on possible risks and to monitor for longer term health effects. A&E departments have not gained explicit consent from those individuals who have provided their personal data information. What should they do?

Outcome: The Data Protection Act 1998 allows processing for the purposes of 'vital interests' (see Case Study 1) as well as for the provision of healthcare (under Schedule 3 of the Data Protection Act 1998). However the common law duty of confidentiality does still need to be taken into account. Where the purpose of data sharing is to protect the health of the individual patient, consent could be implied as there is an expectation that data will be shared with other health professionals for this purpose. Where the purpose is the protection of the health of the wider population, a public interest case must be made for data to be shared without explicit consent.

Where the HPA requires patient information because it wishes to monitor the long term health effects of the accident on the wider population, then it should do so either with explicit consent or, where obtaining consent is impracticable, with support under Section 60 of the Health and Social Care Act 2001.[56] While it could be argued that there is a public interest in disclosing information under the Data Protection Act 1998 to the HPA, since it is required for long term follow-up rather than an emergency response, the use of Section 60 powers would be a more appropriate approach.

---

[54] In making the personal data anonymous the data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the Data Protection Act 1998.

[55] As a real world example from the 7 July 2005 attacks, the Health Protection Agency's requesting form and procedures are available at: **http://www.hpa.org.uk/london_bombings/response.htm**

[56] See paragraph 4.3 of this guidance.

Case Study 8 Scenario: The police are called to deal with a 'white powder' incident in a major postal sorting office. The likelihood that the white powder contains hazardous biological material (eg anthrax spores) is assessed as high. The local NHS and the HPA request details of the nature and extent of exposure in the building and a list of all those potentially exposed. The police have made a list of those in the building for the purposes of the investigation. However, consent to pass personal data on to other agencies so that they can contact them on health grounds was not obtained by the police when compiling their list, and concerns are raised that the details of the nature and method of delivery of the white powder are sensitive with respect to the security response and attempts to detect the perpetrators.

Outcome: There are two aspects to this case study. Firstly, the confidentiality of the information in terms of individual's privacy, and secondly the security implications of passing the information.

Taking the first element (the individuals' privacy), as for case study 1, even though the police do not have consent from the data providers, this does not necessarily mean that the information cannot be passed. The public interest, both in terms of the individuals potentially exposed and the wider public who could be subject to secondary contamination, is very likely to outweigh the marginal cost to individual's privacy.

In relation to the second element (security sensitivity), the police need to assess whether the security implications of passing the information outweigh the benefits to potentially exposed individuals. The outcome will, as ever, depend on the exact details which are released. The security implications could be managed by the police gaining assurance from the NHS and HPA that the information is not placed into the public domain (ie it is not published) and that it is kept securely (which should be the case anyway when sharing). Any particularly sensitive details could also be redacted.