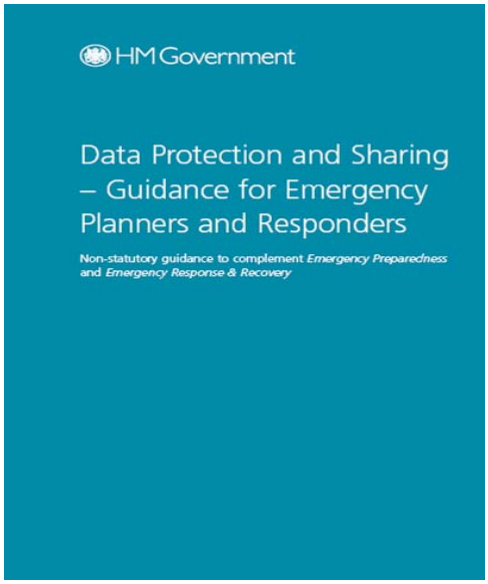
HM Government

Data Protection and Sharing in Emergencies – Guidance for Local Authority Responders

In response to lessons identified from the 7 July London bombings, the Cabinet Office has published guidance on data protection and sharing in emergencies. Problems with data sharing between Category 1 and 2 responders after the attacks hampered the connection of survivors to some support services. Category 1 and 2 responders include **local authorities, health bodies, private sector utility companies and transport operators** amongst others. This guidance can help you to understand and promote your information sharing roles and responsibilities in planning for, responding to and recovering from emergencies.

The guidance provides clear and understandable explanations on the law surrounding personal data so that as local authority responders, you know what can and cannot be done when handling personal data. The **key points** are summarised on the reverse of this sheet - put this up in your office, use the detailed guidance to explore further, and find out the answers to your detailed questions.



You can visit http://www.ukresilience.info/preparedness/informationsharing.aspx to download the guidance. Here you will also find further advice on information sharing and data protection, and the relevant responsibilities placed on local authorities in emergency and non-emergency situations. **This guidance can help you ahead of the next emergency.**

Data Protection and Sharing - 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 test will generally be easier to meet 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 confident in asserting their power to share personal data when lawful 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. As well as the UK Resilience website, the Ministry of Justice offers guidance and a helpline (http://justice.gov.uk , 020 7210 8034).**

- **The Cabinet Office publication "Data Protection and Sharing – Guidance for Emergency Planners and Responders" has been endorsed by the Ministry of Justice, the Information Commissioners Office, the Department of Health, the Local Government Association and the Association of Chief Police Officers amongst many others.**

Further details on information sharing and data protection in emergency and non-emergency scenarios can be found at http://www.ukresilience.info/preparedness/informationsharing.aspx.