|  |  |  |  |
| --- | --- | --- | --- |
| **DO...**  • think before you click and ensure personal data is sent securely using the technology available e.g. 7-zip etc.  • ensure data sharing respects the confidentiality of individuals and there is a data sharing agreement in place with the other party  • consider if the disclosure of personal data is within the reasonable expectations of the individual whose  personal data is involved  • assess that the disclosure, sharing or transfer of personal data is lawful  • make sure you have read and understood the internet and email policies relevant to SGUL and any other  organisations  • post large attachments to secure folders and inform your audience by email of the file location  • scan email attachments for viruses before you open them  • only address emails to people who need to know  • include a relevant title for your email message  • make sure you are aware of confidentiality and data sensitivity issues before sending messages  • be sure that information published on a website is accurate and up to date before using it. | **Principal Investigator Obligations**  **All research and researchers have a duty of care to comply with legal requirements and with SGUL**  **and JRES policies, procedures and guidelines.**  Personal or sensitive personal data must be fairly obtained with all appropriate informed consents.  Transfers of personal or sensitive data outside of the European Economic Area (EEA) must be registered with the SGUL Data Protection Officer, Information Services. The territory should have data protection regulations equivalent to the  UK in place. Failing this a contractual arrangement is required that specifies appropriate information governance obligations for the third party.  Personal data can also be securely protected using encryption,  pseudonymisation and anonymisation techniques.  **Caution Matching Datasets**    If matching with other datasets, take care that importing rare medical conditions, ethnicity and postcode data can  potentially make it personal sensitive data and that the security controls are appropriate. There may be a need  to encrypt or de-identify the data. | **Data Protection Act**  Researchers should be aware that they must comply with the Data Protection Act 2018 and ensure appropriate information security is in place. A contravention of the data protection principles can result in a penalty of up to £17M.  **If you lose personal or sensitive personal data you can face a fine of up to £17M from the Information**  **Commissioner’s Office (ICO).**  **Incident Reporting**  An information security incident involves an event that impacts the confidentiality, integrity or availability of SGUL’s data. All such incidents must be reported to [DataProtection@sgul.ac.uk](mailto:dataprotection@sgul.ac.uk) and the Data Protection Officer. This process will inform the Senior Information Risk Owner and the relevant IG Leads.  The incident must be reported as soon as possible to conform with requirements set by the Information Commissioner’s Office. | **Data Handling:**  A Guide for Research Study Principal Investigators  handling identifiable data  For support email: [DataProtection@sgul.ac.uk](mailto:dataprotection@sgul.ac.uk)  Or  view the [IG Web Pages](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance)  (web – only available internally) |
| **Purpose of this guide**  This guide has been put together to assist research study Principal Investigators  (PIs) handling identifiable data.  Within SGUL, PIs frequently handle large volumes of data received from external organisations much of it of a sensitive nature. We need to ensure that the data is handled in a way that complies with the standards of the information providers and respects the interests and preferences of the research subject.  **Some definitions…**  **Personal data** is any information that can identify an individual.  **Sensitive data** is personal data that can be one or more of the following: mental or physical health; sexual life; ethnicity; religious or other similar beliefs;  trade union membership; political opinions; criminal offences or potential offences committed and any  associated sentence. | **Working with NHS data**  **Identifiable data from NHS patients can be used in clinical research if consent has been obtained with**  **clarity regarding its use, if the organisations which will have access have been identified and if patients are**  **informed that their data will be transferred outside the UK**.  If not the study must apply to the Health Research Authority (HRA) for a S251 exemption. Otherwise the Information  Commissioner could impose a fine of up to £17M.  S251 exemption now requires compliance with the NHS DSP Toolkit. The **NHS DSP Toolkit** is a set of standards for measuring information governance, within SGUL compliance is typically requested by research study teams under the ‘Research /University’  category which measures compliance with 10 data standards.  **Further guidance on gaining NHS DSP Toolkit accreditation can be found at:**  [**SGUL Intranet pages:**](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance) | **Securing Personal and**  **Sensitive Data**  Personal data should be processed in the EEA, if this isn’t possible sufficient measures should be put in place,  **if in doubt check with the SGUL Data Protection Officer.**  **Approved mechanisms for transferring this type of data include:**  • **AES 256-bit encryption or higher** of email attachments using a tool such as **7-Zip** or **WinZip**  • **NHSmail** is secure when both the sender and receiver have a NHSmail address (with the suffix @**nhs.net**)  • **Public key encryption** of emails using a tool such as OpenPGP using **AES 256-bit encryption** or higher encryption  • SGUL IT Services should be contacted in respect of providing secure FTP  services outside of the  SGUL network  Report all information incidents to the SGUL Data Protection Officer  **For further advice and guidance:**  [**SGUL Intranet pages**](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance)**:** | **Dont...**  • ignore the Data Protection Act’s eight principles  • disclose personal data without confirming the identity of the recipient and that they have a justifiable need to know  • send any more personal data than the minimum necessary dataset  • where an alternative is available, send personal or sensitive personal data by fax  • access websites that may contain inappropriate or offensive material  • include personal or sensitive data in the title of your email message  • download files or open email attachments without being absolutely certain that you can trust the sender and  the content  • send large attachments to multiple recipients  • send or forward junk mail, chain letters or virus warnings – these may be hoaxes or dangerous.  **Contact**  Email: [dataprotection@sgul.ac.uk](mailto:dataprotection@sgul.ac.uk) |