Data Protection

Action	Rationale/Comment
Introduction As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard. In the course of its activities InVent Health will collect, store and process personal data, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations. The types of personal data that InVent Health may be required to handle include information about current, past and prospective employees, Commissioning bodies and Local Authorities, patients and their families, and others with whom it communicates. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) and other regulations, including the General Data Protection Regulation ((EU) 2016/679) (GDPR).	The Act imposes restrictions on how InVent Health may process personal data, and a breach of the Act could give rise to criminal sanctions as well as bad publicity.
Status of the Policy This policy has been approved by the Senior Management Team. It sets out InVent Health's rules on data protection and the eight data protection principles contained in it. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data. InVent Health's Data Protection Compliance	The Data Protection Compliance Managers are R

Action	Rationale/Comment
manager is responsible for ensuring compliance with the Act and with this policy. This policy is not part of the contract of employment and InVent Health may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action. Any employee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with their line manager or InVent Health's Data Protection Compliance Managers in the first instance.	Hutchison at Norwich office 07944 783 321 email: info@inventhealth.co.uk Questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Compliance Managers.
Definition of Data Protection Terms **Data** is recorded information whether stored electronically, on a computer, or within paper-based filing systems. **Data subjects** for the purpose of this policy include all living identified or identifiable individuals about whom InVent Health holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information. **Personal data** means data relating to a living individual who can be identified (directly or indirectly) from that data (or from that data and other information in possession of InVent Health. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data, but personal details such as someone's contact details or salary would still fall within the scope of the Data Protection Act 1998.	

Action	Rationale/Comment
Data controllers are the people or organisations who determine when, why and how any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. InVent Health is the data controller of all personal data used in its business. **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following InVent Health's data protection and security policies at all times. **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on InVent Health's behalf. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties. **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned	
Data Protection Principles Anyone processing personal data must comply with the eight enforceable principles of good practice set out in the GDPR. These provide that personal data	

Action	Rationale/Comment
must be: • Processed fairly, lawfully and in a transparent manner. • Collected for limited purposes (specified, explicit and legitimate) and in an appropriate way. • Adequate, relevant and not excessive for the purpose. • Accurate and where necessary kept up to date. • Not kept longer than necessary for the purpose. • Processed in line with data subjects' rights and in a manner which ensures it is secure. • Not transferred to people or organisations situated in countries without adequate protection. • Made available to Data Subjects in accordance with their rights.	
Fair and Lawful Processing The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed by InVent Health, and the identities of anyone to whom the data may be disclosed or transferred.	For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.
Processing for Limited Purposes Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the	**Adequate, relevant and non-excessive processing** Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place. You may only process personal data when

Action	Rationale/Comment
new purpose before any processing occurs.	performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties. You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure all personal data collected is adequate and relevant for the intended purposes. You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.
Accurate Data Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.	Inaccurate or out-of-date data should be destroyed. Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from InVent Health's systems when it is no longer required.
Processing in line with Data Subject's Rights and requests Data must be processed in line with data subject's rights and requests. Data subjects have a right to: • Withdraw consent to processing at any time. • Receive certain information about the data controller's processing activities. • Request access to any data held about them by a data controller. • Prevent the processing of their data for direct-marketing purposes. • Ask to have inaccurate data amended. • Prevent processing that is likely to cause damage or distress to themselves or anyone else. •	

Action	Rationale/Comment
Data Security InVent Health must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. The Act requires InVent Health to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves. Security procedures include: • **Entry controls.** Any stranger seen in entry-controlled areas should be reported. • **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.) • **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required. • **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.	Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows: • **Confidentiality** means that only people who are authorised to use the data can access it. • **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed. • **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on InVent Health's central computer system instead of individual PCs.
Reporting a personal data breach The GDPR requires controllers to notify any personal data breach to the applicable regulator and, in certain instances, the Data Subject.	If an employee knows or suspects that a personal data breach has occurred, the employee should not attempt to investigate the matter. The employee should immediately contact the Data Protection Compliance Managers. You should preserve all evidence relating to the potential personal data

Action	Rationale/Comment
Dealing with Subject Access Requests A formal request from a data subject for information InVent Health holds about them must be made in writing. Employees who receive a written request should forward it to their line manager or a Data Protection Compliance manager immediately. If a member of staff (such as a line manager) receives a subject access request, he or she must verify the identity of any individual requesting data (i.e. do not allow third parties to persuade you into disclosing personal data without proper authorization). The data subject access request should be immediately forwarded to the Data Protection Compliance Managers.	breach. When receiving telephone enquiries, employees should be careful about disclosing any personal information held on InVent Health's systems. In particular they should: • Check the caller's identity to make sure that information is only given to a person who is entitled to it. • Suggest that the caller put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked. • Refer to their line manager or the Data Protection Compliance manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information
Monitoring and Review of this Policy This policy will be monitored and amended as necessary and should be read in conjunction with the InVent Health Privacy Policy.	

Commenced	
Reviewed	
Next Review	