Summary of GDPR Policies

1. Group Policy and Procedure on Access to Records & other Data Subject Rights

Summary

This policy provides guidelines for accessing records and other data subject rights within CareTech Holdings Plc and its subsidiaries. The policy covers various aspects, including subject access requests, who can make such requests, refusal of requests, and information sharing with external agencies. It emphasises compliance with relevant legislation and regulations, such as the Essential Standards of Quality and Safety Regulation, General Data Protection Regulations, and the Access to Health Records Act. The policy also outlines the process for handling subject access requests, including verification of identity and the timeframe for response. Additionally, it addresses requests related to deceased individuals, information sharing in specific circumstances, and procedures for making complaints. The policy aims to ensure the protection of personal information and respect for individuals' rights.

2. Policy and Procedure on Information Security

Summary

The Information Security Policy outlines guidelines and procedures to protect sensitive data within the organisation. It covers access control, data encryption, acceptable use, monitoring activities, backup and recovery, physical security, network security, and incident reporting. The policy emphasises the importance of password security, regular data backups, and secure disposal of confidential information. It also addresses remote access, mobile computing, asset management, and evaluating new information systems. Compliance with the policy is mandatory for all employees to safeguard company data and prevent security breaches. The document provides a comprehensive framework for maintaining information security within the organisation.

3. Policy and Procedure on Data Protection

Summary

The Data Protection Policy outlines the company's commitment to protecting personal data and ensuring compliance with data protection laws. It emphasises the importance of obtaining consent,

securely storing and disposing data, and conducting regular reviews. The policy also covers the need for data protection impact assessments and lawful bases for processing personal information. It highlights the rights of individuals regarding their data, including access, rectification, erasure, and objection. The policy guides handling personal information securely, transferring data outside the UK, and responding to personal data breaches. It also addresses consent requirements for direct marketing, passing information to partners, relatives, or carers, and using social media and personal devices. Compliance responsibilities are assigned to different roles within the organisation.

4. Processing of Special Category Data and Criminal Offence Data Policy

Summary

This policy outlines CareTech Group Holdings Ltd's procedures for processing special category and criminal offence data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The policy covers the definition of special category and criminal conviction data, the conditions for processing such data, and the need for an Appropriate Policy Document (APD). It also describes the data being processed, procedures for ensuring compliance with data protection principles, and retention and erasure policies. The policy emphasises accountability, lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality of data. It concludes with information about the review date of the policy document.

5. Subject Access Request Process

Summary

- Day 1: Forward any written subject access request to the Data Protection Officer at data.protection@caretech-uk.com. The response deadline is 28 days from receipt. Obtain postal and email addresses for verbal requests and forward them to the same email. Inform the relevant manager about service user requests.
- Day 2: The Data Protection Team acknowledges the request, logs it, and verifies identity if needed.
- Legal and Data Protection Officer verify identity and determine required information.
- Redact as necessary and report content queries promptly.
- Day 14: Collation deadline. Send redacted records to data.protection@caretech-uk.com for advice.
- Day 21: The manager sends information via secure email unless an alternative method is requested. Notify Data Protection Team to close the request on the system.

6. Sharing Confidential Information about Service Users and Patients Policy

Summary

Confidential Patient or Service User Information refers to identifiable information about an individual's physical or mental health obtained in confidence and used for their care. This policy ensures compliance with legislation when handling such data. It applies to staff with access to patient or service user information and outlines procedures for sharing requests and respecting data usage decisions. Service users can opt out of sharing their confidential information for non-care purposes. The opt-out covers health and adult social care data within the English health system. It is available to individuals registered on the Personal Demographic Service. Children aged 13 and above can set their opt-out, while proxy individuals can act on behalf of those under 13 or lacking capacity. The opt-out does not apply in certain situations, including explicit consent, public health monitoring, overriding public interest, and legal requirements.