Describe features of manual and electronic information storage systems that help ensure security

To provide high-quality care, care organisations must have access to personal information about the individuals they support. Because this information can be sensitive, it is a legal and ethical requirement that it is stored securely. The best way to ensure the security of confidential information is by storing it in a secure location. This can be done manually or electronically. Manual Storage Methods: Manual storage methods involve using physical documents, folders and shelves to store records. The benefit of this type of storage is that it does not require electricity or power and there are no risks associated with electronic malfunctions. Additionally, manual systems don't have any risk for remote data breaches since they do not use computers or networks to store data which can make them more cost-effective than their electronic counterparts. The drawback is that this form of information management requires more manual labour, time and storage space. Information stored in this way should be secured with keys or passcodes so that only authorised people are able to gain access – these could secure rooms, filing cabinets, drawers or cupboards. Contingency measures may need to be taken to ensure that information is not susceptible to fire or water damage. There will be procedures in place to ensure that people can only access information on a need-to-know basis. Electronic Storage Methods: One of the benefits of electronic storage is that information can be accessed and recorded remotely. Another benefit is that storing data digitally reduces the risk for fire or water damage because there are no physical pieces to the data. One disadvantage associated with electronic storage methods is that data can be hacked due to its reliance on networks and computers which means there are more chances of information being breached. Therefore, it is essential that robust systems and policies are in place to prevent this. Firewalls, antivirus systems and password protection should be used to prevent hacking, cyber-attacks or malicious software from compromising data. Individual employees should ensure that their password details are not shared with others. Regular backups may need to be performed to safeguard against hardware failures. That is kinda obvious and straightforward. Records that are saved electronically can be (and usually are) protected by passwords. I don't think you need a reminder here of how a good password is created. Also, some PC systems only allow access by authorized person sign in with their unique password. Nowadays some computers are not even connected to the Internet to avoid the risk of intervention. If the information is stored manually, not electronically, it can simply be locked away when not in use. There are plenty of possibilities to do that. Having secure systems for recording, storing and sharing information is essential in health and social care settings because we handle sensitive information and must ensure the confidentiality of the individuals that we care for and the colleagues that we work with.To meet these assessment criteria, you must be able to describe the features and demonstrate the practices that ensure data security.A secure system is a way of storing data that only allows access to information by authorised people. This could be a locked filing cabinet or password-protected computer software. Secure systems will also protect data from other risks, such as fire, flood or mechanical/electronic failure.Manual Information Storage (Paper or Hard-Copies)Paper documentation should be stored in a secure place according to your organisation's policies and procedures.This may be in a filing cabinet, drawer or folder that is only accessible by authorised persons. To restrict access, the filing cabinet should have a lock on it or the room that the paperwork resides in may only be entered using a key, electronic code, digital ID badge or biometrics (e.g. fingerprint scanner etc.). These storage areas should also be fire and water resistant to prevent damage and destruction as a result of a disaster.Records should ideally not be removed from the secure storage location, or if they are then procedures must be followed to ensure that they are not left in an insecure area. Paperwork containing personal information should never be left unattended in public areas.When discussing information contained in secure records, it is important that precautions are taken to ensure that nobody is able to overhear the conversation to protect confidentiality.Information that no longer needs to be accessed on a day-to-day basis may be archived in a secure storage facility or shredded/incinerated – policies must be in place to guide the destruction of information.Electronic Information Storage (Computer systems)Records may be kept on computer systems and access restricted to personnel on a need-to-know basis. To comply with data protection legislation, these records may only be accessed using a password.Granular permissions may be used so that only certain senior staff are able to amend records and a digital audit trail should be recorded to track changes – this prevents accidental or deliberate deletion of information.It is important that a staff member's password is not shared with others and that they log out (or lock) their computer when they leave their desk to ensure that others with physical access to their computer are not able to access unauthorised information whilst they are away.The records may be stored on the hard drive of the local computer or, ideally, on a secure networked server or cloud-based location. Regular backups should be performed to safeguard against any potential data loss and the backups should be stored in a separate secure location.It may be your organisation's policy to encrypt files when they are transferred to other devices for extra layers of security. Software such as antivirus and firewalls may be used to ensure the integrity of the computers and networks being used.Practices for ensuring securityAlthough we have talked about some of the practices you should follow to ensure the security of confidential information in your work setting, it is important to highlight that each organisation is different and will have different systems and ways of working. You will need to be familiar with your own organisation's policies and procedures and ways of working to handle information correctly and securely.For example, your organisation may have a policy that all documentation about the individuals that you support be stored on a server and not copied over to a local computer. There may be policies about the use of flash drives or installing personal software on a work-issued laptop.For paper-based systems, information may be colour-coded (e.g. care plans are stored in black lever-arch files and financial information in green lever-arch files). You may need to seek permission before making copies of records and ensure that personal information does not leave the building.All staff should know how to report a breach in security – this will usually be a report to your manager but some organisations may have named information officers. Get Answer to This Module Post New Homework Course- Level 3 diploma in care (RQF)Unit 9 – Promote Effective Handling of Information in Care SettingsL.O 2 – Be able to implement good practise in handling information Do You Need Assignment of This Question We must implement secure recording, storage, and sharing systems in health and social services contexts since we handle sensitive information and preserve the anonymity of the patients we care for and the colleagues we work with. To be assessed according to the evaluation criteria outlined below, you must define the characteristics and show the processes that assure data security.A secure system is a method of data storage that is designed to restrict access to data to only authorized individuals. This might be a lockable file cabinet or computer software protected by a password. Systems protected with a great deal of security will also help safeguard data from other threats, such as fire, flood, or mechanical/electronic failure.The guidelines that are set forth for the proper handling of company paperwork states that your company's paperwork should be securely stored. These most likely are documents located in a file cabinet, drawer, or folder which is only accessed by approved personnel. A file cabinet with a lock on it or in the room where the documentation is located should have been used to restrict access. You must have a key, an electronic code, a digital ID badge, or biometrics in order to get entrance (e.g., fingerprint scanner, etc.).Additionally, these storage facilities should be fire and water-resistant to help prevent the building from being damaged or destroyed due to a disaster.First and foremost, safe storage locations and locations for the removal of records must be kept apart. If this isn't done, sensitive information might be left in an unsecured location. For the general public's safety, any paperwork containing personal information should not be left unattended in public spaces.While discussing information contained in secure records, privacy safeguards must be employed to guarantee nobody can overhear the conversation to safeguard confidentiality. The elimination of daily information processing does not have to be mandated, but this is a matter of policy. When information no longer has to be accessed on a daily basis, it may be stored in a secure storage unit or shredded/incinerated.Get solution of assessment that are approved by CAVA accessors, also get assessment help for all mandatory units of NVQ/QCF level 3 diploma in health & social care. We provide custom assessment help for all NVQ/QCF, RQF, CACHE, and ATHE for all diploma levels, you can also get your assignment done from Cheap assignment writing service UK and students also get Paid thesis assistance UK. We have years of experienced writers who not only provide professional assistance to you but also take care of all your thesis need. Buy Answer of This Assessment & Raise Your Grades Loading PreviewSorry, preview is currently unavailable. You can download the paper by clicking the button above. Data Protection Act 1998 (amended in 2003) – The Data Protection Act 1998 (amended in 2003) is a UK law that was set up to protect people's personal information and who the information was shared with. The act also enables people to make sure that their information is being handled correctly. The 1998 Act replaced and consolidated earlier legislation such as the Data Protection Act 1984 and the Access to Personal Files Act 1987. The Data Protection Act 1998 (amended in 2003) is a legal obligation to everyone who holds information about a person. Non-compliance with the Data Protection Act is a criminal offense. Examples of people who hold information who would have to comply with the Data Protection Act 1987 (amended in 2003) is you're GP, NHS, Private Companies etc. If you're GP was to disclose information about you to your mother or father without your consent this would be going against the Data Protection act which could lead to the GP being prosecuted for committing a criminal offense and being non-compliant. Freedom of information act 2000- This act was created to allow members of the public to access information held about them by different public bodies. For example if the NHS holds information about you under the Freedom of Information Act 2000 you have a right to know what this information is and who it is available to. There are three ways to find out information under this act. Haven't found the relevant content? Hire a subject expert to help you with Understand How to Handle Information in Social Care Settings Hire verified expert You can request this information electronically by sending an email to them from their website or using the contact us section. You can write to the department with a request form or a letter requesting access to the information. You can fax the department to request the information. There may be a charge for the information and you can find details of costs by looking on the public bodies' website, calling them or writing to them. The Health and social Care Act- also has guidelines and legislations on how to handle people information correctly. Care Quality Commission's Guidance about "Essential Standards of Quality and Safety Outcome 21"- Provides you with information on how to handle people information and comply with legislation and laws. The General Social Care Council can also give you information and guidelines on their website about handling people information You can also find out how to handle information by looking at your company policies and procedures manual, looking in your own code of conduct and requesting information from your line manager about how to do this effectively. Q 1. 2 Explain how legal requirements and codes of practice inform practice in handling information? A 1. 2 Legal requirements and codes of practice are guidelines, policies and procedures that everyone has to adhere to in their day to day activities when handling information. The guidelines protect you from committing criminal offenses where it is a legal requirement or from facing dismissal when it is a company's policy or procedure. Legal requirements give you guidance and support when storing and handling personal and confidential information about an individual, it will enable you to store information correctly and safely. Q 2.1 Explain how to maintain records that are up to date, complete, accurate and legible? A 2. 1 A good way of maintaining records is on a computer or in a file that can be kept confidential and kept up to date. Records should be updated each time the individual is seen, either at home or in a clinical setting. Records must always be factual and not an opinion, they must be accurate and legible for others to be able to read. When recording information you must date time and sign the documents in some cases the service user may need to sign them as well. There are many thing that you need to update in the records these include: Date and time of arrival or visit what happened what tasks were completed i. e. washed, dressed, fed, medication Outcome of visit and any requests from the service user. For example if you go and visit a service user and you have gave them breakfast and medication for the day you must state this in the records as the next visitor may give the client breakfast and medication again which could overdose the service user. Q 2. 2 Describe practices that ensure security when storing and accessing information? A 2. 2 There are many different ways to ensure security when storing and accessing information: Passwords on computers enable unauthorised people from accessing records as well as emails Keeping records locked away in a filing cabinet/cupboard with a key that only someone who is authorised to open it has the key. Not leaving notes lying around to be seen by anyone Make sure that handovers are done in a room where no one can hear Making sure conversations with service users are in private and not breeching confidentiality. Not discussing information with people on the telephone or if you do doing this in private so no one else can hear. Making sure files are returned to the filing cabinets when not in use. Q 2. 3 Describe features of manual and electronic information storage systems that help ensure security? A 2. 3 It is important to keep all clients information in a secure location (i. e. filing cabinet for paper based records etc.) if any records are taken out of the secure location to be used in updating or retrieving information from they are to be kept away from unauthorised users. For example if you visit a service user in the morning but no longer need their records it should be put in the secure location out of reach of others who are not authorised to use this. Electronic records are to only be accessed by a password which will stop unauthorised people accessing the records. Electronic systems will also record who, when and what time the records have been accessed and what the person was doing when accessing the information. For example is Joe blogs record needed updating to say he was on a new medication. You would log into the computer and put a password into the files to allow you access the computer system would record who you are and what time you accessed the file and what you did with the file. (I. e. amended information, updated records etc.) Always making sure there is a backup of document paper documents should be photocopied and stored in a filing cabinet that is labelled. Electronic records should be backed up either on a USB stick or a server to make sure records are not lost. Q 3. 1 Explain how to support others to understand the need for secure handling of information? A 3. 1 Ways to support others and making them understand the need for secure handling of information is by following policies and procedures yourself which shows good practice. Showing people policies legislation and procedures about handling information and monitoring the way they handle peoples information and offering them guidance and advice on how to handle peoples information in the most secure way meeting the legislation that is in place, advise them to read the data protection act and the companies code of conduct. We all have a duty to follow the procedures and legislation for handling information. If someone does not know how to do this you can show them how to do so, as well as showing them how to update information where required. Q 3. 2 Explain how to support others to understand and contribute to records? A 3. 2 You can support other by raising their awareness of the consequences of not updating records, making them legible and not following policies and procedures in compliance with data protection. Make sure that you colleagues know where to keep secure files and how to store them. (I. e. alphabetically.) Haven't found the relevant content? Hire a subject expert to help you with Understand How to Handle Information in Social Care Settings Hire verified expert