ACMEDICALSERVICES

Data Protection Policy

Introduction

This policy illustrates AC Medical Service Ltd.'s commitment to the safety of patient information. By adhering to the referenced guidance, employees ensure that data and information are protected, which reduces the risk of information security incidents.

AC Medical Services Ltd. Ensure that they comply with General Data Protection Regulation (GDPR) and The National Data Guardian's (NDG) ten data security standards.

Data Security Standards

The purpose of the standards is to enhance existing data security principles, thereby improving data security across the healthcare sector. The standards outline the value of safe, secure, appropriate and lawful sharing of data.[3]

The Data Security Standards are:

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through Blue stream Training.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyberattacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyberattacks are to be reported to CareCERT immediately following detection.

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

Summary

The preservation of data and information security is crucial to maintaining the trust of the patients at AC Medical Services Ltd. All employees are aware that they have a duty to ensure that they handle information correctly and safely, in accordance with extant guidance and in line with the data security standards.