DiCEMark

What organisations tell us about Safety and Quality

This page explains what organisations tell DiCE when they apply to use the DiCEMark. It helps you understand the checks and standards that relate to their services.

The DiCEMark is a quality scheme led by the digital healthcare industry. Digital healthcare uses technology, such as apps or online services, to support care. DiCE reviews information and statements from organisations against the scheme's requirements.

A declaration is a statement that an organisation makes about meeting a requirement. Some requirements only apply to certain services. A declaration does not, on its own, mean an independent check has taken place.

1 Keeping Care Safe and Following the Rules

Organisations must show how they manage risks to patients. They must describe the safety arrangements that apply to their service. These include:

- Clinical safety standards DCB0129 and DCB0160. These standards help organisations find and reduce risks from health technology. DCB0129 covers organisations that make the technology. DCB0160 covers organisations that introduce and use it. Organisations describe how they follow the standards where these apply to their role and service.
- Clinical Safety Officer. This is a trained health professional who helps manage risks from health technology. Organisations provide details of this role where it applies.
- Clinical risk management. This means finding things that could harm patients and taking steps to reduce the risk. Organisations explain how they review these steps regularly.
- Medical devices and MHRA registration. Some health products, including some software, count as medical devices. The Medicines and Healthcare products Regulatory Agency (MHRA) regulates medicines and medical devices in the UK. Organisations state whether their product is a medical device and give registration details where needed. Registration alone does not mean the MHRA has approved the product.
- Remote prescribing guidance. This is guidance on prescribing medicines without meeting the patient in person, such as by video or online. Organisations that provide this service declare that they follow the guidance that applies to them.

2 Protecting Your Personal Information

Organisations provide information about how they protect and use personal information, such as your name and health records. This includes:

- Information Commissioner's Office (ICO) registration. The ICO oversees data protection in the UK. Organisations state their registration status. Registration alone does not show that they meet all data protection rules.
- Data Protection Officer. This person advises on data protection and checks how the organisation follows the rules. Organisations explain their arrangements where this role is required.
- Data Security and Protection Toolkit (DSPT). This is a way for organisations to assess and report how they protect information. Organisations tell DiCE their toolkit status.

- Data Protection Impact Assessment (DPIA). This is a check for risks to your privacy when personal information is used. It helps organisations plan how to reduce those risks. Organisations explain their arrangements for the products and services that need this check.

3 Keeping Technology and Accounts Secure

Organisations explain how they protect their systems from attacks and test how well those systems work. This includes:

- Cyber Essentials and Cyber Essentials Plus. These schemes assess protection against common online attacks. Cyber Essentials Plus also includes independent technical tests. Organisations state which certification they hold, if any.
- External penetration testing. An outside specialist tests systems, with permission, to find security weaknesses. Organisations explain these tests and other steps they take to keep systems secure.
- Multi Factor Authentication (MFA). This adds another check when someone signs in, as well as their password. Organisations explain its use for accounts with extra powers, such as accounts used to change system settings.
- Access audit trails and auditing. These are records of who accessed a system and what they did. Organisations explain how they keep and check these records.
- Load testing. This tests how a system works when many people use it at once. Organisations explain their testing arrangements.

4 Making Websites Accessible

Organisations state how their website meets the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. These guidelines help make websites usable for disabled people. For example, they cover using a keyboard and tools that read text aloud.

5 Having Insurance and Trained Staff

Organisations declare that they have insurance suited to the work they do. Insurance can help cover costs if something goes wrong, depending on the policy.

They also confirm that staff have the training and skills needed for their work. They keep training records up to date and provide refresher training.

6 Other Checks and Certificates

Organisations provide details of other checks that apply to their products or services. These include:

- Digital Technology Assessment Criteria (DTAC). These are NHS criteria for assessing digital health products. They cover safety, privacy, security, working with other systems, and ease of use and access. Organisations state their assessment status where relevant. DTAC is an assessment framework, rather than a single NHS product approval.
- ISO certifications. These show that an organisation has been certified against a named international standard. The standard may cover an area such as quality management or information security. Organisations give details of the certificates they hold.
- Other accreditations and quality checks. Organisations give details of other schemes or checks they use to support quality.

What this information means for you

DiCE can share a summary showing that an organisation has completed the relevant DiCEMark review. The requirements that apply depend on the organisation's role, product and service.

The DiCEMark does not mean that every organisation holds every certificate listed here. It does not replace checks or rules set by regulators. It cannot guarantee that a service is free from risk.

We do not publish private details about individuals, professional registration numbers or detailed security information.

Who is responsible for the information

A person authorised to act for the organisation confirms that its information is correct and complete, as far as they know. They also agree to tell DiCE about relevant changes.