Reference:	FOI.18302.25
Subject:	Cybersecurity standards
Date of Request:	8 September 2025

Requested:

1. **Current Certifications**
   Please disclose which national or international cybersecurity standards the organisation currently holds a formal certification for. This should include, but is not limited to, standards such as Cyber Essentials (CE), Cyber Essentials Plus (CE+), IASME Level 1 & 2, and ISO/IEC 27001.

2. **Welsh Government Directives**
   Kindly specify any national or international cybersecurity standards for which the Welsh Government has formally mandated or requested certification from your organisation. This pertains to recorded communications, contracts, or policies where such a directive is explicitly stated.

3. **Historical Certifications**
   Provide details of any national or international cybersecurity standards to which the organisation was previously certified, but for which the certification has since lapsed or expired. For each expired certification, please include the corresponding expiry date.

4. **In-Progress Certifications**
   Please detail any national or international cybersecurity standards for which the organisation is currently undertaking the certification process.

5. **Assessment Outcomes**
   Disclose whether the organisation has failed any formal assessments for national or international cybersecurity standards. If a failure has occurred, please provide the name of the standard and the date of the failed assessment.

Response:

Hywel Dda University Health Board (UHB) has applied an exemption under Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) as it has deemed that the information requested is exempt from disclosure as it would be likely to prejudice the prevention or detection of crime and potentially increase the risk of cyber-crime. The UHB has also considered the “mosaic effect”; the harm which will or will be likely to arise from the release of this information, when utilised alongside information already in the public domain.

Section 31 of FoIA is a qualified exemption requiring public authorities to apply the public interest test set out in Section 2(2)(b).

The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

The UHB has therefore considered the following:

In favour of disclosure: The UHB has a duty to maintain openness and transparency in all its activities, including decision making, which will help to maintain public trust in the UHB. Disclosing

Cyber security arrangements could provide assurance to the public that the UHB has a robust IT infrastructure in place, which in turn would reassure the public that their information is safe, and that public money has been well spent to ensure this.

Against Disclosure: A disclosure made under the FoIA, is a disclosure to the world at large and by releasing the requested information, the UHB would be vulnerable to it being used for crime. Such action could compromise the security of UHB systems and both patient and staff information, whilst causing disruption to the flow of information through the UHB systems, impacting on patient care and safety.

The UHB takes its Data Protection information governance responsibilities very seriously and has robust arrangements in place to protect its IT systems and infrastructure. Disclosure of this information would reveal how to undermine systems, with the potential need to implement disproportionate steps resulting in additional expense to the public purse, to counter an increased risk that is currently managed.

Decision: Disclosing the information regarding the UHB's Cyber Security certification will likely provide attackers with valuable information regarding the capability of the UHB's Cyber Security. Such a disclosure would enable targeted research that would compromise the integrity and confidentiality of its systems which contain sensitive information. The UHB has also taken into account the wider context of significant and growing cyber threats and attacks which continue to present a substantial risk to the world at large.

There is a clear public interest in protecting society and the UHB from the impact of crime. Therefore, the UHB has concluded that the public interest in withholding the information is greater than the interest in disclosing, consequently protecting the UHB from potential criminal activity.