UKRI policy fellowships 2026

Fellowship position

Fellowship title:

UKHSA cyber security fellowship

Fellowship type:

Core policy fellowship

Host organisation:

UK Health Security Agency (UKHSA)

Host team:

Cyber Security team, part of the Chief Data Officer (CDO) group.

Academic discipline/s:

Computer science, artificial intelligence, data science, cyber security and data analytics

Summary:

Strengthening the UK's Health Security by protecting vital data and insights from advanced AI cyber threats, building an evidence-based foundation for coordinated national policy.

Policy topic:

IS-8 Sectors - Digital and Technologies, Life Sciences; Professional and Business Services

Research career stage:

Open to early and mid-career researchers

Fellowship structure

The fellowship is estimated to begin in May 2027. The exact date will be confirmed by the host depending on onboarding and security clearance requirements. The fellowship will have three phases:

- inception: duration is 3 months at 0.4 FTE
- main placement: duration is 12 months at 0.6-1 FTE
- knowledge exchange: duration is 3 months at 0.4 FTE

Work arrangements

Location requirements:

The fellowship position will be offered as remote based with the option for attending offices more frequently if the fellow wishes to. There will be some travel required to our head office at 10 South Colonnade, Canary Wharf, London to attend team meetings/away days at least once a month to enable greater team working. The successful fellow will also be able to attend our offices in Liverpool, Leeds and Birmingham, as desired.

Hybrid working:

The fellowship will be remote/hybrid based with occasional office/event attendance, but this is at the successful candidate's discretion.

Security clearance and nationality eligibility criteria:

Please refer to the following links which provide guidance on the nationality criteria for the civil service Civil Service recruitment: nationality rules - GOV.UK.

Basic Personnel Security Standard (BPSS) will be required, which usually takes around six weeks. We would expect the successful applicant to start the security clearance application process, with support from the host team, as soon as their fellowship has been confirmed by UKRI. Inception phase can begin before the security clearance process is completed but will be required for the main placement phase. Please see National security vetting: clearance levels - GOV.UK for more information.

It would be beneficial for the fellow to have security clearance to work in the Cyber Security team which could take up to 6 months, so this will be started at the earliest confirmation of the successful fellow. This will not impede on the start date of the fellow as long as they have secured BPSS, the fellow can undergo the security clearance whilst in their placement. For more information please visit the following link and read the applicant guidance SC - Guidance Pack for Applicants - GOV.UK.

Fellowship position description

The UKHSA is the nation's expert body for health security, responsible for preparing, preventing and responding to infectious diseases and environmental hazards. As an executive agency of the Department of Health and Social Care (DHSC), UKHSA provides scientific and operational leadership to protect public health and enhance national preparedness. Proprietary datasets, AI/ML models, and analytics pipelines now underpin growth across UK industry but face escalating threats, including model theft, dataset poisoning, supply chain compromise, and cloud-based intrusion. We envisage the fellow to generate one or more of the following outcomes: actionable policy frameworks, improved protection of critical health data, and stronger analytical capability across UKHSA and its partners.

This project will assess risks to high value data and analytics intellectual property and develop policy recommendations to strengthen resilience across strategic sectors. As organisations rely more heavily on data driven decision-making, attackers increasingly target underlying datasets and models, causing economic loss, distorted insights, and reduced competitiveness. With no cross-sector UK framework for protecting analytical IP, the fellow would have a great opportunity to contribute to building an evidence-based foundation for coordinated national policy. They will be embedded in the Cyber Security team and have access to internal systems of high sensitivity (if security clearance is obtained) this will enable an in depth understanding of the policy and cyber security processes and cross-government setup. For someone interested in a career in Cyber Security this would be a great stepping stone to achieving that, giving them the opportunity to shape real impactful work for the UKHSA.

Co-design and collaboration will be embedded from the inception phase of the fellowship. The fellow will play an active role in shaping the project's direction, focus, and outputs in partnership with the host team and relevant stakeholders. During the inception phase, the fellow will contribute to defining research questions, methodologies, and success measures, ensuring alignment with both organisational priorities and their own research interests. This collaborative approach will continue throughout delivery via regular engagement with internal teams and partners. This model ensures the fellowship is co-developed rather

than pre-defined, enabling the fellow to meaningfully influence the scope of work and develop outputs that reflect both organisational needs and independent academic interests.

The fellowship would deliver significant impact by supporting UKHSA's ambition to strengthen cyber resilience across the health security ecosystem. The fellow would be involved in the codesign of the inception phase, collaborating to develop a national threat model for data and analytics IP, produce cross sector guidelines for securing data assets and AI models, and generate policy proposals on standards, incentives and regulatory focus. The fellow would also enhance collaboration between industry, academia and government, creating a sustained pipeline for knowledge exchange. There will be opportunities to present to local teams within UKHSA, or cross-government and to academic networks to foster collaborations. The fellow will have autonomy to create the path they want to explore with this work, mapping out their objectives with the Cyber team during the inception phase, therefore if the fellow has a particular research interest this could be explored during this phase to incorporate into the wider project.

The fellow will be provided with an Academic Honorary Contract with UKHSA, with a line manager in the organisation and an induction, IT equipment, email address and access to relevant systems will be organised in accordance with the relevant security checks being completed.

The fellow will have opportunities to work on site at any of the UKHSA locations including London – Canary Wharf, London - Colindale, and regional offices across the country as well as working remotely.

The fellow will be part of the Chief Data Officer's Group in UKHSA, who have a track record in research publication, engagement with academia, engagement with policymakers and use of evidence to inform policy, practice, and guidance. Here are some other benefits the fellow will have from working within UKHSA, and specifically in the Cyber Security team:

- be fully embedded into a Division (Cyber Security) and will have the opportunity to interact with a wide range of experts within UKHSA and with our partner organisations.
- the fellow will have the opportunity to produce and publish original research, ensuring that findings contribute to wider scientific and policy discussions, while adhering to necessary security protocols.
- support will be provided from UKHSA to facilitate the publication of open access journal articles and support from experienced researchers to develop and publish outputs from research projects.
- opportunities to present to local and national teams within UKHSA, and cross-government and academic networks to foster collaborations and raise awareness of their work.
- crucially the Fellow will have full exposure to the incident management arrangements of UKHSA, a health protection and health security-focused Category 1 responder.

The fellow will also join CDO's Early Career Researcher Network which brings other placement students from a variety of schemes together to meet regularly. This network was set up to not only develop a community culture but to bring learning and development opportunities to ECRs from across the agency. We encourage the fellow to champion their own learning and development, branching outside of their respective team, building their professional network and collaborative skills.

Person specification

Applications will be assessed by UKRI panel assessment against the following essential opportunity-specific requirements in addition to the generic eligibility and call criteria.

Essential criteria:

- basic understanding of cybersecurity principles, including threat detection, incident response, or vulnerability management
- familiarity with at least one information security framework (e.g. MITRE ATT&CK, NIST, or ISO 27001)
- exposure to query or data analysis tools (e.g. KQL or similar), or willingness to learn

Applicants shortlisted from the panel assessment will be invited to a host led interview. At this stage the host will also consider the following desirable fellowship-specific requirements:

Desirable criteria:

- postgraduate study or relevant certifications in cybersecurity, AI, or policy-related fields
- exposure to research, academic writing, or policy analysis

Processing personal data

If applicants are shortlisted by the UKRI assessment panel UKRI will need to share the application and any personal information that it contains with the host for the host led interview selection process.

Your personal data will be handled in line with UK data protection legislation and managed securely. If you would like to know more, including how to exercise your Rights, please see the UKRI privacy notice.

Please see Host's privacy notice and they will delete your data at the end of the selection process unless you are successful, in which case we will retain your data as an independent data controller.