NIHAP
Data Analytics Platform
DELIVERING CARE TOGETHER

Department of Health | An Roinn Sláinte | Männystrie O Poustie

NI Health Analytics Platform- Information Governance Guidance and Checklist for Controller Organisations

This guide and checklist has been developed to assist organisations who wish to use NIHAP to ensure appropriate information governance considerations in relation to their processing and management of information on the platform. It also highlights the responsibilities of organisations as data controllers of any personal data they process on the platform.

Organisations must ensure they use the platform appropriately and that they have the correct information governance and data protection in place to ensure that they meet their legal obligations under relevant legislation, including UK General Data Protection Regulation (UKGDPR) and the Data Protection Act (DPA) 2018, (referred to as UK Data Protection Law).

All organisations that decide to process personal data on NIHAP are data controllers for that data. The Department of Health (DoH) will act as a processor on behalf of controller organisations in delivering the platform, providing systems administration and in some cases providing analytics expertise and support. The Department will also be a controller of any identifiable data it is directly responsible for on the platform and relevant Departmental Information Asset Owners (IAOs) must ensure they follow this guidance also.

All organisations must consult with their IG leads in advance of processing on NIHAP.

All organisations must ensure they put in place a Controller- Processor MoU with DoH- (HSCDI)- before processing personal data on NIHAP. The HSCDI have developed a template to assist organisations and will provide this at the outset of discussions with the NIHAP team. This MoU will set out the data protection obligations and roles and responsibilities of each party. It will also help to ensure compliance with UK Data Protection Law.

Checklist

Before processing data on NIHAP:

Action
Consult with your Information Governance Lead/ Data Protection Officer (DPO) and Personal Data Guardian (PDG) about your processing on NIHAP and have received their advice and input into all actions below.
Ensure that all personal data processing on NIHAP complies with UK GDPR and DPA 2018, with particular focus on ensuring compliance with the UK GDPR Article 5 Principles relating to the processing of personal data.
Provide relevant privacy notices/ update privacy notices to data subjects to inform them about the processing of their personal data on NIHAP by your organisation.
Carry out Data Protection Impact Assessments in relation to the processing of personal data on NIHAP and have identified and implemented appropriate mitigations for any risks identified. (The NIHAP team can provide input in relation to processing activities they may carry out on your behalf. They can also provide the NIHAP DPIA for the platform to provide relevant information about security of the platform etc, which may inform your project specific DPIA).
Put in place a Controller-Processor MoU with DoH, (or update any existing MoU to account for new processing), using the available template, which should be formally reviewed by your DPO before submitting to the NIHAP team.
Ensure that retention and disposal is applied to the data you process on NIHAP, in line with the retention and disposal schedules set out in Good Management, Good Records (GMGR) and that processes are in place to action appropriate disposal and deletion of information from NIHAP when required, in line with GMGR schedules.
Ensure that all staff processing data on NIHAP have completed up to date Information Governance training, which includes data protection; (this includes any third parties working on your behalf, including contractors or students etc).
Ensure that data is processed in compliance with the common law duty of confidentiality and the DoH Code of Practice on Protecting the Confidentiality of Service User Information.
Ensure that all staff processing personal data on NIHAP are aware of their duties of confidentiality and that their duties in this regard are part of their employment contracts, or equivalent; (this includes any third parties working on your behalf, including contractors or students etc).
Ensure appropriate security (organisational and technical) is in place to prevent any security threat to NIHAP as a result of your organisations access to NIHAP. All organisations must comply with either NICS or HSC IT Security policies.