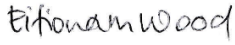# Bangor University Healthcare Research Theme Information System-Level Security Policy and Working Practices

Centre for Health and Medicines Evaluation (CHEME),
School of Healthcare Sciences, Bangor University

Version:	4	Issue date	26/04/21

Author	Position	Signature	Date
Eifiona Wood e.wood@bangor.ac.uk	Senior Research Fellow, CHEME, Bangor University	*Eifionam Wood*	26/04/21
Approved by:	**Position**	**Signature**	**Date**
Gwenan Hine Gwenan.hine@bangor.ac.uk	Senior Information Risk Office (SIRO) and Data Protection Officer (DPO) Bangor University	*Gwenan Hine*	26/04/21
Dyfrig Hughes d.a.hughes@bangor.ac.uk	Professor of Pharmacoeconomics, CHEME, Bangor University	*(signature)*	26/04/21

Revision History		
Version Number	**Revision Date**	**Reason for revision / What was changed**
2	May 2018	Updated to NHS Digital SLSP template 2018
3	January/May 2019	Updated policy links & SIRO (David Thomas)
4	April 2021	Updated policy links & author and approvers New section on Remote Working

Contents

Abbreviations

PID   Patient Identifiable Data
DPO   Data Protection Officer
HES   Hospital Episode Statistics
SIRO   Senior Information Risk Owner

1. Introduction

The Centre for Health Economics and Medicines Evaluation (CHEME), within the School of Health Sciences, Bangor University undertakes health economic evaluation activities in association with clinical and research departments across the UK. This document is a requirement of the NHS Digital Data Sharing Framework Contract which needs renewal on an annual basis in order for staff in the School of Health Sciences to be able to handle patient level data supplied by the NHS Digital in the form of Hospital Episode Statistics (HES) data and other data types such as prescribing data. HES data is an integral component essential to the conduct of these activities and CHEME therefore requires access to this data. CHEME takes responsibility for the safe import, processing, storage and destruction of HES records.

2. Scope

This document covers the technical and physical system-level security requirements for the handling of data relating to NHS Digital and Hospital Episode Statistics (HES) data protection within the School of Healthcare Sciences. These policies are to be used alongside Bangor University IT security and data protection policies which can be found at:

https://www.bangor.ac.uk/governance-and-compliance/policy-register/index.php.en

The School of Health Sciences system sits within Bangor University's dedicated research computing service, a suite of resources which provide technical and physical controls for the storage, sharing (if applicable) and analysis of research data.

3. System Details

3.1. System design
The System is the complete data handling solution for any aggregate data relating to NHS Digital and Hospital Episode Statistics (HES) data protection within the School of Health Sciences, Bangor University. It relates to the safe import, processing, storage and destruction of HES data in accordance with the requirements set out by NHS Digital and policies of Bangor University.

- The Senior Information Risk Owner is Gwenan Hine, Head of Governance Services, Bangor University
- The System's Data Protection Officer (DPO) is Gwenan Hine, Head of Governance Services, Bangor University

3.2. System security
Security of the system shall be governed by Bangor University's Information Governance Policies:

- Data Protection Policy https://www.bangor.ac.uk/governance-and-compliance/dataprotection/documents/Data-Protection-Policy-approved-v7-June-2020.pdf
- Information Security Policy and Guidelines https://www.bangor.ac.uk/governance-and-compliance/policy-register/documents/information-security-policy.pdf and https://www.bangor.ac.uk/governance-and-compliance/InfSecGuid.php.en

Patient identifiable / sensitive data

- Data import is performed by authorised university staff as and when required and access granted according to pre-defined sharing agreements paying particular attention to the latest version of the data protection and confidentiality SOP of the clinical trial unit (CTU) or similar patient study unit with which we are working.
- All personal identifiers are removed at source and data is identified solely by a trial randomisation number or a patient study identity number. Unless specific provision is made beforehand, NHS Digital should always be consulted to ensure no patient identifiers or other potentially sensitive fields (e.g. pseudohesid from HES data) are in the dataset.
- Master lists linking participant personal details to the randomisation number or patient study identity number are restricted and should only be handled by authorised staff defined in the study protocol.
- Data will have all patient identifiable information removed when it comes to CHEME and will only be identified at the patient level via the trial randomisation number. Information will be held on an encrypted laptop and flash drives and once work on extracting data is completed it will be shredded using HMG IS5 via active Kill disc at a time to be agreed with NHS Digital.

Data processing

- Data is not permitted to leave the secure server once uploaded unless specifically authorised within the Trial or Study Management Group and done in accordance with the trial or study protocol.
- Only users authorised by Trial or Study Management Groups, or the Data Controller will have access to the data and will process it in a way to aggregate the data to provide estimates of cost-effectiveness of the trial intervention. This will typically be the trial health economist or other users authorised by the data controller. We do not anticipate greater than 3 individuals having access to HES data per project – the main trial health economist, the principal health economist investigator and up to one further support researcher to lend advice on handling HES data.
- Aggregated anonymised data are allowed to be exported from the systems only once risk assessments have been carried out to ascertain compliance with avoidance of deductive disclosure due to small cell sizes (e.g. to comply with data sharing agreements with data providers such as the NHS Digital or the Office of National Statistics). Typically, a formal risk assessments will be needed when data is broken down into geographical areas or small groups (e.g. in the case of a potentially sensitive area as STIs it would mean reporting 4 in a population of 10,000 as <5).
- Extraction of HRGs and costing of HRGs will be performed by trial health economists at an anonymised patient level.
- The information extracted will be aggregated at a patient level to show HRGs used and associated costs over the trial period. This will be incorporated into a dataset which will be held on Bangor University central drive; this data will be at randomisation number level only with no patient identifiable details included. The HRG information extracted will be used to supplement information from other sources and compiled and aggregated to give average resource use and average costs for the different trial arms and so will not be published at an individual patient level.
- Typical outputs from School of Health Sciences include for example cost-effectiveness estimates, cost-effectiveness planes, cost-acceptability curves, mean costs of treatment by intervention, mean units and costs of resource use, mean clinical outcomes (eg life-years gained, quality adjusted life years) and coefficients derived from regression analyses.

Responsibilities

- The System shall be developed by qualified staff and approved by the Data Protection Officer in conjunction with the IT department.
- The System shall be implemented by the Data Protection Officer (DPO) and maintained by the Senior Information Risk Owner (SIRO).
- The System shall be not shared or used by other organisations.

Data Protection Officer (DPO)
- The ultimate responsibility for data protection compliance rests with Bangor University's Head of Governance Services who delegates operational control to the Senior Information Risk Owner (SIRO). This responsibility includes, as far as is reasonably practicable, the provision of adequate resources to meet the requirements of the policy.
- The DPO has overall responsibility for protecting the confidentiality of PID. The DPO plays a key role in ensuring that the organisation and partner organisations abide by the highest level for standards for handling PID and adherence to the Caldicott Principles.

Senior Information Risk Owner (SIRO)
The SIRO is Gwenan Hine, a member of Corporate Services within Bangor University with allocated lead responsibility for the organisation information risks and provides a focus for the management of information risk. The SIRO is accountable for:
- Fostering a culture across the organisation for protecting and using data.
- Providing a focal point for managing information risk and incidents.
- Monitoring activities relating to policies and procedures to be followed by all staff and recognising actual or potential security incidents.

The CHEME NHS Digital designated contact will take responsibility for ensuring all staff receive the relevant training and keeping updated training logs.

Physical and Environmental Security
Bangor University provides to the School of Health Sciences the following system resources:-

Physical access to building
- Physical access to the building is controlled outside of working hours by keycard for authorised staff. Access during working hours is monitored by CCTV.
- Individual offices are locked when unattended during and after working hours.
- All key holders are approved by the DPO.

Electronic data access
- The School of Health Sciences benefits from centrally provided services from the University's IT Services department as well as some of its own resources managed by its own research staff.
- Access to any NHS Digital data will be from using equipment that has been supplied by Bangor University IT Department which is fit for purpose and is compliant with Bangor University Information Governance and Security polices and NHS Digital security assured PCs.
- Access to the computer system will only be granted to staff, who have unique User IDs and passwords to securely access the system.
- A secured file storage area operated from a Microsoft Windows file server platform. The area is secured by the use of access control lists based on a tightly controlled group of authorised users.
- General networking provision both internally and to the wider internet which is managed by a perimeter firewall device.
- VMW are virtualised environments that allows bespoke servers to be run on shared hardware. Access to the virtualised hardware is tightly controlled, access to the actual guest operating environment is delegated to the department requesting the virtual server. Where IT Services manages the entire virtual environment the guest operating is expected to be a RedHat Linux derivative or Microsoft Windows.
- Data held within central systems (both file storage and virtual environment servers) is backed up stored on a single encrypted disc within a dedicated card-controlled machine room.

- Changes to the provision and configuration of these services as well as changes requested to individual user permissions are logged and managed through an issue tracking system and enacted by IT Services authorised staff.
- Monitoring of resources utilisation and access to these environments is also undertaken.
- No mobile devices will be used to access this information.
- Remote access to computer systems will only be granted to designated staff approved by the SIRO

Removable Media
- Although data is hosted within a secure server, and securely accessed using user ID and password authentication, it may be necessary to receive removable media from data providers. All removable media can only be handled by staff authorised by the study protocol.
- The designated researcher may receive the following removable media
  - CD/DVD disks
  - Solid-state memory devices
- Once transferred to a secure server, these media must be stored in a lockable cabinet or safe in a secure lockable room. Removable media is kept for a minimum period of 5 years unless specified otherwise in the study protocol or by the NHS Digital.

Clear Screen and Desk Policy
- All users are required to disconnect their session when leaving their workstation/terminal by logging out of or locking their computer.
- On returning to their desktop, users must re-log into their computer by typing their user ID and password to gain access to the system.
- Users are not permitted to transcribe any sensitive information contained within the secure system onto any other information system or paper record nor are they allowed to use digital imaging technology to capture all or part of the output from a screen or monitor.

Remote working
- All staff currently and as long as relevant to do so follow Bangor University policy and guidance on working from home https://www.bangor.ac.uk/humanresources/policies/documents/InterimHomeworkingPolicy_000.pdf and https://www.bangor.ac.uk/itservices/working-off-campus.php.en. In addition all staff follow the Data Protection policy and Information Security policy with regards to remote use of IT resources, cloud computing and remote accessing of university drives.

Data storage
- All data will be kept in accordance with Bangor University Records Management Policy https://www.bangor.ac.uk/governance-and-compliance/documents/Records-Management-Retention-Policy-2019.pdf,   University Record and Data Retention Schedule https://www.bangor.ac.uk/governance-and-compliance/UniRetSched.php.en, Information Security Policy https://www.bangor.ac.uk/governance-and-compliance/policy-register/documents/information-security-policy.pdf and Information Security Guidelines https://www.bangor.ac.uk/governance-and-compliance/InfSecGuid.php.en

- All documentation and paper records containing the data is kept in a locked cupboard and when no longer required are micro cross cut shredded to HMG Infosec S5 DIN Level 4/5 on site prior to disposal using the Bangor University specialist certified waste disposal contractor who collects the confidential material, confidentially destroys it and provides certificates of destruction.

- Any electronic data when required to be deleted, will ensure that it is multi pass wiped to at least HMG S5 using for example ActiveKilldisc software on site following Bangor University Guidance on

the Destruction of Records Containing Confidential Data https://www.bangor.ac.uk/governance-and-compliance/dataprotection/DestConfData.php.en

- If end of life, the storage unit will be degaussed and physically destroyed and securely disposed of following Bangor University 'Policy for the Re-use and Disposal of Computers, other IT Equipment' https://www.bangor.ac.uk/itservices/disposal-policy.php.en

End of studies

- Any electronic data when required to be deleted, will ensure that it is multi pass wiped to at least HMG S5 using ActiveKilldisc software on site following Bangor University Guidance on the Destruction of Records Containing Confidential Data https://www.bangor.ac.uk/governance-and-compliance/dataprotection/DestConfData.php.en

- If end of life, the storage unit will be degaussed and physically destroyed and securely disposed of following Bangor University 'Policy for the Re-use and Disposal of Computers, other IT Equipment https://www.bangor.ac.uk/itservices/disposal-policy.php.en

- All documentation and paper records containing the data is kept in a locked cupboard and when no longer required are micro cross cut shredded to HMG Infosec S5 DIN Level 4/5 on site prior to disposal using the Bangor University specialist certified waste disposal contractor who collects the confidential material, confidentially destroys it and provides certificates of destruction.

3.3. System Audit
The System shall benefit from the following audit arrangements:

- The System will be risk assessed and audited every 12 months.
- The risk assessment will ensure that current practice is complete and fit for purpose so to understand what information it holds and what security arrangements are necessary in order to protect such information from any security breaches and whether such arrangements are actually put into effect.
- The audit will ensure that, that all staff are qualified, trained and aware of patient confidentiality issues, that up-to-date records staff training have been maintained and that any personal data which they hold, whether in electronic or paper format, is kept securely, in accordance with SLSP, the General Data Protection Regulation and Research Ethics Committee approved processes.

3.4. System Protection
The System shall benefit from the following resilience / contingency / disaster recovery arrangements.
- The SLSP will be saved on a remote server that can be accessed from any internet enabled computer.
- No backups of the NHS Digital data will be kept at Bangor University. Aggregated data for analysis and reporting in journals will be kept on Bangor University central drive with access limited to authorised users.
- Backup of data stored on Bangor University School of Health Sciences central drive secured networked shared area is performed nightly and stored on a single encrypted disc within a dedicated card-controlled machine room.
- All electronic data is encrypted to the standard in which it is given by the data supplier.

4. System Level Security Policy Ownership

- The SLSP shall be the responsibility of the SIRO.

- The SLSP shall be available / distributed to all staff in electronic form. The SLSP will also be available on the Bangor University School of Health Sciences website.

5. Data Protection Registration

Bangor University has Data Protection Registration no: Z7439647

6. Supporting Documents

Information Governance Documents
Bangor University Corporate Governance polices for the technical and physical controls employed to enforce the following detail:

Data Disposals/Destruction Policy	https://www.bangor.ac.uk/governance-and-compliance/dataprotection/DestConfData.php.en
Password Policy	https://www.bangor.ac.uk/itservices/good-password.php.en
Mobile Computing Policy	https://www.bangor.ac.uk/itservices/mobile-devices/index.php.en
Acceptable Use Policy	https://www.bangor.ac.uk/itservices/policies/accept_use.php.en
Compliance Policy	https://www.bangor.ac.uk/governance-and-compliance/governance.php.en
Software Management Policy	https://www.bangor.ac.uk/itservices/policies/accept_use.php.en
System Management Policy	https://www.bangor.ac.uk/itservices/policies/accept_use.php.en
User Management policy	https://www.bangor.ac.uk/itservices/policies/accept_use.php.en
Network Management Policy	https://www.bangor.ac.uk/itservices/policies.php.en
Information Handling Policy	https://www.bangor.ac.uk/itservices/policies.php.en
Physical Security Policy	
Data Protection Policy	https://www.bangor.ac.uk/governance-and-compliance/dataprotection/index.php.en
Remote Access policy	https://www.bangor.ac.uk/itservices/policies/accept_use.php.en
Back and Recovery Policy	
Incident Response Policy	https://www.bangor.ac.uk/governance-and-compliance/dataprotection/index.php.en
Virtual Private Network (VPN)	
Guest Access Policy	
Anti-virus Software Policy	https://www.bangor.ac.uk/itservices/anti-virus.php.en
Wireless Policy	https://www.bangor.ac.uk/itservices/policies.php.en
Third Party Connection Policy	https://www.bangor.ac.uk/itservices/policies.php.en

Network Security Policy	https://www.bangor.ac.uk/itservices/policies.php.en
Encryption Policy	https://www.bangor.ac.uk/itservices/protect-data.php.en
Cloud Security Policy	https://www.bangor.ac.uk/itservices/policies.php.en
Confidential Data Policy	https://www.bangor.ac.uk/itservices/policies.php.en https://www.bangor.ac.uk/governance-and-compliance/governance.php.en
Data Classification Policy	
Retention Policy	https://www.bangor.ac.uk/governance-and-compliance/documents/Records-Management-Retention-Policy-2019.pdf https://www.bangor.ac.uk/governance-and-compliance/UniRetSched.php
Outsourcing Policy	
Network Topology	

7. Review and Revisions

This policy will need to adapt to changing circumstances and will therefore be kept under annual review and revised as necessary. Responsibility for revising and updating the policy lies with CHEME. Revised policies will be submitted to the SIRO for approval and review.