BSW ICR & PHM – Information Security statement

This statement is designed to give an overview of the key security features and operations of the Integrated Care Record and Population Health Management. The organisations providing these controls should be assessing the effectiveness of these on a regular basis (GPDR Article 32 – Security). This does not cover the processing by BSW CCG to extract and prepare general practice data for upload as that is separately covered by the data processing agreement between the CCG and each practice.

ICR PHM data processors (all to be listed here):

- Graphnet Health Ltd (https://www.graphnethealth.com/)

Security area	Overview of controls
Personnel security	
Vetting	*All partner organisation and data processor staff are subject to employment references and background checks.* **Graphnet -** Confirmed in Graphnet contract Annex 2 – Security Statement **ICR Partners** – part of employment processes
Education & training	*All staff (data processor employees and end users) undertake both induction and annual information governance related training. Common commitment for all staff to read and be able to access their employing organisation's information governance policies.* **Graphnet** – All staff receive annual Information Governance and Information Security Training as well as all new starters receiving additional training when they start in the Organisation. **ICR Partners** – confirmed by DS&P toolkit. Compliance is a requirement of signing the Data Sharing Agreement
Employment contracts	*Confidentiality contractual clauses in place – linked to disciplinary action for all parties.* **Graphnet –** Confirmed in Graphnet contract Annex 2 – Security Statement **ICR Partners** – confirmed by DS&P toolkit
Physical security – related to data centre (not end user access points)	
Security perimeter	*Data Host – Facilities are assessed to meet requirements of ISO27001. CCTV coverage is in place.* **Graphnet** – ISO27001 confirmed in Contract Schedule C. Statement of applicability also provided. Microsoft Azure cloud facilities also meet these standards and NHS Cloud services requirements
Physical entry controls	**Graphnet –** The office Building operates via swipe card access. There

	are two layers of security to the shared building complex. The first allows access to the Building and the second allows access to the Graphnet office. All members of staff and visitors sign in and out. Visitor passes are available to guests once they have signed in and been appropriately greeted by a member of staff. Azure Data Centre access itself is controlled by Microsoft.
Environmental protection (fire, flood, theft)	Data storage must be on dual sites with immediate fall over in the event of issue at one site. **Graphnet –** The solution supports geo-redundancy using multiple data centres which are configured in either an active-passive, or active-active model.
Secure disposal of equipment	*Data Centre devices at 'end of life' or that fail are securely retained on site until physically destroyed onsite by an accredited disposal company under supervision of Data Processor. Certificates of destruction are issued.* **Graphnet** – As per above.
Data Centre & data processing locations	*All data centres used are NHS Digital approved data centres. All data centres are UK based. All data processing will be conducted within the UK by UK based staff.* **Graphnet** – Contract Schedule F confirms use of Amazon Web Services and Microsoft Azure cloud server, approved NHS Cloud providers, with data centres in the UK. Our contract assures that no Data Controller's data would be processed outside of the EU (with additional commitment from Graphnet that no data will be processed outside of the UK).
Communications & Operations management	
Separating development, test and live facilities	*Test, development and live environments are segregated. Test data is not taken from the live environment.* **Graphnet** – confirmed in ISO27001 applicability statement (A 12.1.4)
Anti-virus/malware	*Anti-virus and malware protection is in place on the infrastructure and operating systems provided by Data Processors.* **Graphnet –** The solution is protected by Microsoft Defender, Microsoft Anti-malware and Azure Security Centre.
Backups and continuity – Business continuity	*Redundancy for all power systems (Generator & UPS) in data centres. Data is stored at one Data Centre and is replicated to a second Data Centre.* **Graphnet** - Graphnet performs nightly back-ups 365 days per year as part of normal operations. All back-ups are stored, for a period of 30 days, in machine readable data on an industry standard medium at a site remote from the data centre or systems location and shall be available within 30 minutes for online/disk backups and 4 hours for offsite stored tape media for the purposes of data retrieval. Backups

	are tested, standardised and shared with the customer on the requirements.
Network security & testing/auditing	• *Data centre subject to annual (or more frequent as required) penetration testing, carried out by CESG CHECK certified external assessors.* **Graphnet** - Microsoft fully manages its Azure hosted Cloud. Microsoft carries out regular penetration testing to ensure safety from security vulnerabilities. • *Virtual Private Networks (VPN) and Virtual Local Area Network (VLAN) established in the host centre.* **Graphnet** - Already built into Azure is Azure Advanced Theft Protection. The network will be monitored for vulnerabilities and deviation from original configuration statues (routes). Changes to the network layout will be fully audited. Any changes are only accessible via Just In Time administration built on top of multifactor authentication to ensure only the authorised personnel can make changes. • *Vulnerability scans are conducted at least quarterly. Daily checks of incoming vulnerability disclosures, Common Vulnerabilities and Exposures (CVE) reporting. Security patches applied in a non-production environment first where possible.* **Graphnet** – Microsoft Azure has built in vulnerability assessment abilities providing holistic protection that will be constantly monitoring the stack. All security patches are delivered to non-production environments first.
Encryption & Pseudonymisation	Transit Layer Security (TLS) utilised (CESG approved products). Data is also encrypted at rest (AES 256). Laptops and other mobile devices used for access to ICR will be encrypted. Delivery of the system to the device accessing it is via Secure Socket Layer (SSL 2048 bits) at all times. Wireless traffic is encrypted using WPA2 Pseudonymisation is not used in terms of delivery of care to identifiable individuals, but will be used in population health management platform. **Graphnet –** TLS encryption confirmed in ISO27001 statement of applicability (A 13.2.1). Mobile devices are encrypted (A 6.2.1). Data is encrypted at rest using TDE (Transparent Database Encryption).
Monitoring	
Audit logging & Usage audits	*Audit logs are in place for all aspects of the ICR system and the infrastructure on which it is run. ICR captures all User ID, date and time stamp for all interactions on the system, including records of who viewed data.* *Monitoring for security events or incidents (i.e. failed logins) are in*

	place. All partner agencies will conduct usage audits to ensure that access to data is for appropriate valid reasons. **Graphnet –** Audit logs are in place across the system and All audit logs and evidence is preserved to ensure appropriate chain of custody.
Access control	
User management	A user request process and form will be established. This will require organisational manager approval before the user is set up. Set up of users will be delegated to their employing organisation following a standard process to ensure only valid accounts are created. The employing organisation will also be responsible for any required changes or removal of access and will link the relevant procedures to their overall starter/leaver processes to ensure swift creation, update and removal of access. User is identified by email address and password. NB 'context launch' users who access the system from their core business system will be subject to their local access request/approval processes.
User access control definition	**End user access control –** All access managed via the 'need to know' principle applied at the system, function and data level via Role Based Access, Landing Pages and function access control. Unique username & password access control (either via 'context launch from core business system or 'portal' access). User profile and access to data is 'role based' and 'task based', linked to employing organisation. **System administration access** at all levels is all based on the principle of least privilege and segregation of duties where possible. Log of allocated access privileges is monitored.
User responsibilities (passwords, equipment, clear desk/screen	*All data processor staff are trained as part of their IG training on workstation security, this includes clear screen/desk, locking workstations when not in use etc.* **Graphnet** – Password Management, clear screen and desk is regularly reviewed on audits and spot checks by the Compliance and Governance Managers. There are posters in the building to remind staff as well as the areas forming part of annual training.
Password management	Lockout is activated after 5 unsuccessful login attempts. Access is then frozen for 15 minutes. Password complexity – minimum 8 characters, mix of alpha numeric

	& 42 day renewal period. Cannot use previous 5 passwords **(NB not applicable where context launch from users source system is enabled – the standard on that system will apply)** CareCentric provides password management that can be configured to meet local preferences, such as: Expire Account Inactivity Days; Logon Failure Count Before Account Locked; Max Password Age; Force of Alphabetic and/or numeric, special characters; minimum length, time out intervals and previous passwords remembered.
Session Time out	After a period of non-use (15 minutes) the user is locked out until they successfully re-identify to the system. **As above**
Incident reporting and management	In terms of reporting personal data breaches, the responsibilities are covered in the Information Sharing Agreement between the partners participating in the ICR/PHM programme. Graphnet – Contractual obligation to notify of incident is in place. All staff are trained on the importance of their own responsibilities to be aware of any incidents and to raise up. There is an identified group of appropriate staff who will assist to review and manage any identified incident. Graphnet utilises Jira to review any incidents which links and logs issues to ensure the incident is managed within the internal policies and processes.