Issue 4: October 2018

Black Country Partnership NHS Foundation Trust

Data Protection Newsletter

Joint Working within the Black Country

Special points of interest:

- Data Protection Training Dates now available across the Trust
- The Trust continues to work towards increasing compliance with data protection
- Audits are being rolled out to monitor compliance

The Trust is working with partners across the Black Country to ensure that everyone receives streamlined care.

The Trust is continuing working with partners to ensure data is shared appropriately and securely to ensure that our clients receive high quality care from multi-disciplinary teams across Wolverhampton, Walsall and the MERIT Partnership.

The Trust's Health Visiting Service has been working with the Local Authority and Vacc UK to ensure that children have access to vaccinations and immunisation programs.

The Trust has also been working with Dudley and Walsall Mental Health Trust to review our current electronic patient record systems to implement a new system which will streamline information sharing within services to ensure that patient information is available to all clinical staff who are involved in their care throughout the Trust.

Information Governance Team is working with services in relation to the implementation and roll out of the new electronic record system.

Inside this issue:

Cyber Security Accreditation Achieved

We are pleased to announce that the Trust's IT department recently undertook an exercise to become a nationally accredited organisation in the realms of computer security.

The Government backed Cyber Essentials scheme is managed by the National Cyber Security Centre and aims to give organisations the peace of mind that their defences will protect against the vast majority of common cyber-attacks, because the attackers are looking for targets which do not have the Cyber Essentials technical controls in place.

Qualification for the accreditation follows a rigorous application and evidence gathering by independent auditors, and we now intend to work towards achieving 'Cyber Essential Plus', which is compulsory for all NHS organisations to achieve before June 2021.

Further information is available via the Cyber Essentials website.

Our Community
you matter, we care

Data Protection Training

The Information Governance (IG) Team continue to deliver training across the Trust.

New Training dates will be announced shortly for the Data Protection Training from January 2019 onwards. Although there are no bookable training courses advertised at present staff can still access training via e-learning. In addition services can book training to be delivered directly to their service/teams, during which a member of the IG Team will be available following the training for any service specific issues or questions linked to Data Protection.

Please note in addition to the Data Protection Training the IG Team also provides the following internal training packages:

Freedom of Information; providing an overview of Freedom of Information and the process taken for requests for information.

Information Governance Training; which includes Data Protection awareness which includes individual's rights, Freedom of information awareness, information security and guidelines for information sharing.

NHS Staff Survey

Your information is not shared or included as part of the Staff Survey results.

The annual staff survey has now been circulated. This year they are being sent electronically. All surveys will be delivered electronically to your in-box.

We are aware that some staff do not complete the survey because of issues around confidentiality.

Please be aware that the Trust will not know who has responded to the survey and will not know individuals responses. Quality Health runs the survey on behalf of the Trust; and provides assurances around confidentiality, although they know who they contact for surveys your personal data, such as your name, is not attributed to the response and the only information they share is the responses.

If you have any queries about the staff survey please contact one of your local trade union reps for support.

New Policies Launching Soon

The Trust has reviewed the current Information Governance Policies in line with legislative change. This has led to all of the policies and procedures being updated and a new Data Protection and Information Security Policy being produced.

All policies have undergone consultation with both corporate and clinical staff being represented as part of this. As before the policies have been designed to be easy to follow with key pages that can be printed and used as posters within the SOPs.

Once made live the policies and procedures will be available on the Trusts intranet site and will also be available to the public via the website.

The key changes within the policies and procedures that staff must be aware of are linked to:

- Patient rights
- Subject Access Procedures
- Information Security

Right to be Forgotten

GDPR provides individuals eight rights in relation to their data. One of these rights is the 'Right to Erasure' otherwise known as the right to be forgotten.

This means that individuals can request organisations to delete information that is held about them.

This request can be made verbally to any individual within the organisation and must be acted upon.

Requests received by the Trust for erasure of records may not be fully adhered to. Although the right to erasure is a fundamental right, it must be applied sensibly.

There are legitimate areas under the GDPR where processing can lawfully continue and such a request refused.

Medical Records is an example of information that cannot be erased as they will be required for the ongoing care and treatment for individuals. Where an individual has been fully discharged from services Medical Records are secured in archive and destroyed in line with the Trusts retention and destruction schedules.

Staff are the first line of defense

All good information governance practices start with our staff. It is vital that all staff understand their responsibilities to protect data.

There are a number of tips that the Information Governance team ask all staff to follow, these are:

- ✓ Check staff's ID prior to allowing access to buildings.
- ✓ Ask people who are not normally in the building who they are and what they are doing here.
- ✓ Ensure doors and cabinets are locked
- ✓ Escort visitors throughout the building
- ✓ Lock your computers when away from your desk
- ✓ Follow Clear Desk Policy
- ✓ Do not write passwords down.

All staff are responsible for the security of information

Realities of getting Data Protection wrong

A former NHS Nurse has been prosecuted in September 2018 for accessing patients' medical records without authorisation. She had inappropriately accessed the records – including maternity and paediatric records - of five patients, 17 times.

The former Nurse made multiple accesses to the records of some of these individuals including the blood results of a friend 44 times after they had been discharged.

This case has come after another similar case where an NHS receptionist had been prosecuted, in April 2018, for accessing patient records without authorisation.

The former receptionist inappropriately accessed the records of 12 patients outside of her role as receptionist / general assistant. She pleaded guilty to unlawfully accessing personal data and unlawfully disclosing personal data.

Each of these cases resulted in the staff members being dismissed from their job roles. Each also received fine's in addition they had to pay victim surcharges and costs.

The Trusts policies and procedures are there to protect you as well as the information we hold. Staff must follow these to prevent such breaches happening.

ico.
Information Commissioner's Office

Good Practice Areas

Pond Lane, Wolverhampton

A recent Information Governance Audit was carried out at Pond Lane, Wolverhampton. The Audit was to review progress against concerns over security which were highlighted within previous audits. Although there are constraints on what measures could be put in to place due to the design of the building it was clear that staff were doing all they could to maintain security and confidentiality. Due to staff the audit showed that all information and assets were secured (locked behind at least two levels of security); confidential information was not left on desks when staff were away from their desks. Staff ensured that people within the building are escorted appropriately and had valid ID badges.

Jamie Woodall, Business Intelligence

Jamie is the Freedom of Information Lead for the Business Intelligence Team, as part of his role he collates information in line with FOI requests within a tight deadline. It is vital that corporate data is also viewed with a data security and protection stance as not all personal data is stored within the Trusts Health Records; Jamie does this as part of his FOI role.

As well as being aware of the Freedom of Information Act 2000, Jamie must be aware of the data protection requirements in relation to releasing information that has the potential to identify an individual. Carly Tully, IG & FOI Lead for the Trust, has identified that Jamie always delivers the information for requests on time and correctly identifies where relevant exemptions are required, linked to Data Protection, to ensure that data is protected appropriately.

Who to Contact for Further Information

Katie Sparrow, Head of Information Governance and Data Protection Officer

Email: Katie.sparrow@nhs.net
Tel: 0121 612 8017

Subject Access (access to information) Requests
Email: bcpft.infogov@nhs.net
Tel: 0121 612 8037

Freedom of Information Requests
If you want to know more about how the Trust is performing in relation to GDPR please forward your questions to: bcpft.foi@nhs.net