Issue 5: December 2018

Black Country Partnership NHS Foundation Trust

Data Protection Newsletter

Data Protection Myth Busting

Special points of interest:

- Data Protection Training is still available on request from the IG Team
- The Trust continues to work towards increasing compliance with data protection
- Audits are underway in relation to Data Protection compliance

"He's making a list,
He's checking it twice,
He's gonna find out who's naughty or nice,
Santa Claus is in contravention of Article 4 of the General Data Protection Regulation (EU) 2016/679."

The above rewriting of the popular Christmas song has been doing the round and has even been picked up by the ICO! However Santa doesn't need reporting to the IC Ho Ho Ho...

We have noticed that there are still a lot of misconceptions in relation to Data Protection and even Records Management across the Trust. So we have tried to address some of these throughout this article.

Some of the myths we have heard are:

- We cannot report incidents to the police due to the need to disclose patient data.
- Students can NEVER use our patient records as part of their supervision or studies
- We cannot share patient's information with non-NHS organisations, such as Local Authorities, without consent.

Inside this issue:

Consent Myth Buster

The Trust does not generally process (or use and share) data based on the consent of the service user.

The Trust provides details of our data processing, how we use information, via our website and leaflets, in addition to this services are required to make the service user aware of how they use and share information. It is important to be open about who we will share information with, however we do not require consent to do so. If the patient raises concerns with sharing with a particular individual / organsiation then this must be documented within their notes and where possible adhered to.

If you have any queries in relation to the use of existing consent forms or consent in general please contact the Information Governance Team.

Good Records Management = Good Data Protection

Part of Data Protection is ensuring good records management.

Principle 3 highlights information should be adequate, relevant and limited to what is necessary. This links to records management to ensure that the information is recorded within the correct locations to ensure that the relevance is noted for the service. In addition principle 4 highlights that information must be accurate and, where necessary, kept up to date. The accuracy of data is linked to the time taken to record and file information within the records. Information must be recorded within 24 hours of the consultation or event to ensure that vital information is remembered. In addition information must be stored within the file once available as this must be accessible to the correct staff at the point that this is required.

Accessibility of records falls part of the overall record management processes within the Trust which includes how records are stored within our service areas, tracked when out of storage and archived once no longer required.

The Trust's Record Management Policies are available on the Trust's website or staff intranet pages.

Can we share data?

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

The biggest myth around Data Protection is that it stops people being able to share data.

Data Protection legislation does not prevent data from being shared where there is a legitimate reason for the sharing of information. However it does put rules in place to ensure that the information is shared for the correct purposes (or legal basis) and is shared securely; for example via encrypted means if electronic.

The seventh principle of Caldicott supports this by highlighting the need to weigh up the reasons for and against disclosure of information. If the reasons and/or risks weigh more in favour of disclosure then the information should be shared via secure methods.

Further information and support about sharing information is available from the Trust's IG Team.

New Information Governance Policies

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.

The Policies and Procedures are now live and available on the Trust's intranet site and are publically available via the Trust's 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 Restrict Processing

GDPR provides individuals eight rights in relation to their data. One of these rights is the 'Right to Restrict Processing'.

This gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that the Trust uses their data. This is an alternative to requesting the erasure of their data.

Such requests can be made verbally or in writing and all requests received by the Trust must be clearly documented within the individual's records.

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

Where an individual has restricted the processing of their data and there may be a risk to the individual, or another person, by adhering to the request, then the information may need to continue to be processed.

Where a request has been made staff can seek advice from the Trust's Data Protection Officer or Information Governance Team; all contact details are available within the end of this newsletter.

Be Cyber Aware!

Good Cyber Security means good information governance practices. Although IT Service ensure that Cyber Security is applied within the Trust, all staff have a responsibility to maintain cyber security practices.

There are a number of tips that the Information Governance and IT Services Teams ask all staff to follow, these are:

- ✓ Use the Lock Screen function
- ✓ Use lock print function.
- ✓ Use secure passwords which are not easily guessable and are not written down.
- ✓ Ensure USBs or other removable media items are obtained from IT Services to maintain encryption standards
- ✓ Encrypt emails sent outside of secure domains
- ✓ Recognise Phishing Emails, report these and do not open any links.
- ✓ Lock away mobile devices when not in use.
- ✓ Be careful what you click – avoid unknown websites or downloading software from untrusted sources.

All staff are responsible for the Cyber Security

Joint Working across Governance Assurance

The Governance Assurance Unit (GAU) consists of the following areas:

- Information Governance
- Patient Safety and Compliance
- Health and Safety
- Security
- Patient Engagement
- Patient Experience
- Research and Innovation
- Litigation and Claims

GAU is the synchronisation of all of these areas in to one central team which compliments each other.

GAU provides support with staff across the whole Governance Agenda. GAU supports the divisions to implement and monitor their risk, safety and governance framework.

GAU provides assurance to the Board that the Trust is compliant with statutory regulations and is managing and monitoring risk and governance across all services.

GAU also ensures necessary safeguards for patient and corporate information are in place and that information is used appropriately.

GAU works together to ensure that services and patients are supported within any process throughout the Trust. GAU ensures that the patient voice is heard through various methods. GAU is a central resource that can be accessed by all staff.

Good Practice Areas

Records Management Group Re-established

The Trust has re-established the Records Management Group within the Trust. This Group ensures that both Health and Corporate Records are managed appropriately across all areas. The Group will provide assurances in relation to the storage, transfer and content of records which is set to maintain high standards and improve Record Management compliance across the organisation, which will also underpin the Trust's Data Protection and Freedom of Information compliance.

Increasing Security on Mobile Devices

The ICT Services Team has proven to be Cyber Security Alert and is constantly improving the security around the Trust's electronic devices. The Team proactively monitors the Trust's cyber security and where weaknesses are identified they put in solutions to ensure that the Trust's data is secure. In November ICT Services strengthened the security on all Trust mobile phone devices by enhancing the password requirements so that staff was mandated to use an approved password format, thus reducing the risk of phones being inappropriately accessed.

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