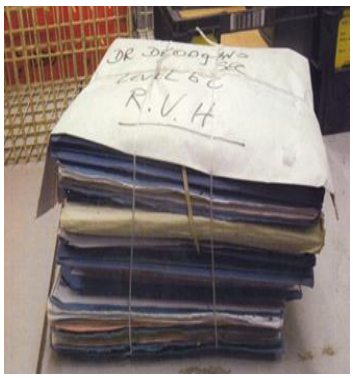
# INFORMATION GOVERNANCE Bulletin

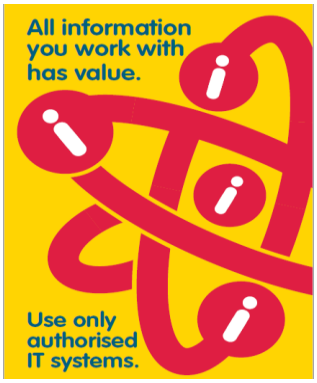
Bulletin
June 2021
Issue 27

Contact us for any Data Protection concerns, including requests for erasure, correction or for data breaches. Reportable breaches must be notified to the ICO within 72 hours via the Information Governance in the Trust. For complaints relating to the processing of personal data, the Information Governance Department may need to respond directly to complainants - **seek our advice!**

## Inside This Issue






IG Posters to Download

## Freedom of Information – 20 working days – clock is ticking.

The Public Liaison team within the Corporate Communications Directorate provides a central point of contact for Freedom of Information requests. The team aims to provide accurate and timely responses, within 20 working days or sooner, to meet legislative requirements.

Should you receive an FOI request, please contact the Public Liaison team immediately. The Trust has 20 working days to answer starting from the date the request was received into the organisation - so time is of the essence!

For a request to be valid under FOI it must be in writing, but requesters do not have to mention the Act or direct their request to a designated member of staff. If you receive a request, make sure it goes quickly to the Public Liaison team: publicliaison@belfasttrust.hscni.net. You can give us a call on: 028 9504 5888 for advice and assistance.

## Preservation of Trust records

1. Virtual Archive Training is now available through MS Teams – for more information contact Deirdre.Allison@belfasttrust.hscni.net

(If your name is already on the WL, no need to make contact as you will receive an email invite directly)

2. 'Pack It Tight To Send It Right' campaign launched in 2015 still applies!

Patient records should be secured within a tamperproof envelope, addressed appropriately and contain 'sender' details on reverse.

## Sending encrypted emails to external users – FORTIMAIL (replacing SOPHOS)

The Region have changed the system that is used to send encrypted emails to external users.

**Impact to internal users sending encrypted email**: None – users that wish to send encrypted email to an external user continue to use the same method by typing [ENCRYPT] in the subject line of the email.

**Impact to external users receiving encrypted email:** Whenever external users now receive an encrypted email, they may need to re-register on the new secure portal that will be sent along with the email. If they have issues accessing the new portal, they will need to contact their own IT department to resolve.

The new portal uses port 4443, which may be blocked by some firewalls. The documents here can provide them with further instructions.

Any further issues should be logged to BSO Service Desk by emailing supportteam@hscni.net or by phone at 02895362400. Current information on the Hub is to be updated however, there are some documents here that may be of use to external recipients.

http://intranet.belfasttrust.local/directorates/par/it/Documents/Receiving%20Encrypted%20Mail%20-%20Windows%2010%20User.pdf

http://intranet.belfasttrust.local/directorates/par/it/Documents/Receiving%20encrypted%20email%20-%20iPadiPhone.pdf

## Document Storage and Sharing within Microsoft Teams

With COVID-19 putting digital dependence at front and centre of the healthcare sector, Belfast Trust embraced technology and found new ways to work.

Staff rapidly adjusted to working remotely. Social distancing rules meant replacing the majority of face-to-face meetings and contact to online. Microsoft Teams provides us with a platform for secure collaboration and healthcare tools in a single location.

When collaborating and sharing information, staff need to be data security conscious and ensure access is configured appropriately. Access and sharing of information should be configured using least privileged access. If good governance is not regularly reviewed and maintained there is an increased risk of data breaches occurring.

Team Site Owners

- Your Microsoft Team should be restricted to only relevant staff involved, this access should be reviewed and maintained to reflect staff leaving, changing role etc.
- Confidential files and documents should only be shared when the necessary restrictions have been configured – ask yourself who needs to see this? Use secure channels, providing access to only those who need. This is especially important if you have members from outside Belfast Trust configured with guest access to your Team.
- If in doubt when saving or sharing documents do not proceed without seeking advice from ICT or the Information Governance Team.

### Need More Information?

**Contact:**

**General Manager HSC Records**
PatriciaM.McAteer@belfasttrust.hscni.net
Tel: 028 95048207

**Data Protection Officer:**
Gillian.Acheson@belfasttrust.hscni.net
Tel: 028 95046955

**Asst Data Protection Officer:**
Cathy.Cole@belfasttrust.hscni.net
Tel: 028 9504 6925

**Information Governance Manager:**
Hilary.Waugh@belfasttrust.hscni.net
Tel: 0289504 6641

**Subject Access Requests (community):**
DataProtection@belfasttrust.hscni.net
or global list as DataProtection-SM or
Tel: 028 95046955

**Subject Access Requests (Acute):**
medlegalservs@belfasttrust.hscni.net or
global address MedLegalServs-SM or
Tel: 028 95 040726.

**Acute Records**
Cathrine.Rogan@belfasttrust.hscni.net
Tel: 028 95 047664

**Corporate Records (Community Services)**

Deirdre.allison@belfasttrust.hscni.net
Tel: 028 95047002

### Training Available On

Data Protection
Redaction of records
Archiving Records
Access to Records
Data Breach - Incident Management

**Contact**
**dataprotection@belfasttrust.hscni.net**
**for more info.**

**To download our IG Posters Click HERE**


Team Site Members

- If you have inappropriate access to information, especially if it is confidential or sensitive, you should immediately notify the Team owner and contact the Information Governance Team to inform them of the breach.
- All data breaches should be recorded as an incident within DATIX.
- Never verbally or digitally share information that you should not have access to or to any individuals that also should not have access.
- Only ever access information that relates to you and your work.

These same principles apply across any platform when providing access or sharing and consuming information. If in doubt always ask advice first.

## Ransomware – what is it, and why do we need to be vigilant?

Ransomware is a malicious application (malware) employed by criminals to target individuals and organisations. Once injected into your computer it encrypts all of your data, documents and emails and then locks you out of your PC; the only way to get data and files back is to pay the ransom to the hackers. What makes ransomware particularly destructive is that once the malware gets onto a device, it then attempts to replicate to other PCs and servers and will ultimately attempt to encrypt all BHSCT devices – you can just imagine the clinical disruption this would cause in BHSCT.

In recent months QUB have been the victim of a sophisticated ransomware attack, and only last weekend the HSE suffered a significant ransomware compromise and is currently experiencing major clinical disruption. Ransomware demands can be significant; the current HSE ransom demand is rumoured to be 20 Million euro.

Ransomware is everywhere, so staying vigilant and follow the recommendations:

1. Keep up to date: Regularly updating programs and operating systems helps to protect you from malware. When performing updates, make sure you benefit from the latest antivirus & security patches. This makes it harder for cybercriminals to exploit vulnerabilities in your programs.

2. Never click on unsafe links: Avoid clicking on links in spam messages or on unknown websites. Avoid visiting non-corporate websites where possible.

3. Avoid disclosing personal information: If you receive a call, text message, or email from an untrusted source requesting personal information, do not reply. Cybercriminals who are planning a ransomware attack often try to collect personal information to allow them to customise an email to make it appear more genuine, and increase the likelihood of you clicking an embedded link.

4. Do not open suspicious email attachments: Ransomware can find its way to your device through email attachments. Avoid opening any dubious-looking attachments. To make sure the email is trustworthy, pay close attention to the sender and check that the address is correct. Never open attachments that prompt you to run macros to view them. If the attachment is infected, opening it will run a malicious macro that gives malware control of your computer.

Useful ransomware Links

https://www.ncsc.gov.uk/files/Phishing-attacks-dealing-suspicious-emails-infographic.pdf

https://www.ncsc.gov.uk/files/staff_training_infographic_3.pdf