eMBED HEALTH CONSORTIUM

# *Information Governance Newsletter*

*Issue 3*


## Be aware when using bulk email

**Addressing Bulk Email appropriately**

Does your job involve contacting groups of patients or members of the public through a single email?

If it does please ensure you are aware of the correct method to do this i.e. through the use of 'blind carbon copy' or BCC. If you use the 'copy to' or cc function you could be breaching the confidentiality of the individuals you are sending information to and as a result the Data Protection Act, which can lead to monetary penalties for your organisation.

**Remember**

Remember to use BCC when sending bulk emails to patients, engagement group members or other members of the public in order to protect the confidentiality of those individuals

The above also applies if using a pre-set distribution lists, with the added need to check that all addressees included in that list are entitled to receive the information being disclosed.

Be careful when using the 'reply to all' function, should the information you have added be sent to all those in the original email, will the reply cause the details of those who were originally included in a BCC email to be disclosed?

Be careful not to disclose any personal identifiable information in the email itself

Be aware of the 'email trail'. There may be additional information further down the body of the email which should not be shared / forwarded to the bulk email addresses.

## In this issue…




**ICO fines Uber £385,000 over data protection failings**

The Information Commissioner's Office (ICO) has fined ride sharing company Uber £385,000 for failing to protect customers' personal information during a cyber-attack.
A series of avoidable data security flaws allowed the personal details of around 2.7million UK customers to be accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company. This included full names, email addresses and phone numbers.
The records of almost 82,000 drivers based in the UK – which included details of journeys made and how much they were paid – were also taken during the incident in October and November 2016. The ICO investigation found 'credential stuffing', a process by which compromised username and password pairs are injected into websites until they are matched to an existing account, was used to gain access to Uber's data storage.

However, the customers and drivers affected were not told about the incident for more than a year. Instead, Uber paid the attackers responsible $100,000 to destroy the data they had downloaded.

# Bupa fined £175,000 for systemic data protection failures

Bupa Insurance Services Limited (Bupa) has been fined £175,000 by the Information Commissioner's Office (ICO) for failing to have effective security measures in place to protect customers' personal information.
Between 6 January and 11 March 2017, a Bupa employee was able to extract the personal information of 547,000 Bupa Global customers and offer it for sale on the dark web.

The employee sent bulk data reports to his personal email account. The compromised information, which included names, dates of birth, email addresses and nationality, was later offered for sale on the dark web.

# Gloucestershire Police fined for revealing identities of abuse victims in bulk email

Gloucestershire Police has been fined £80,000 by the Information Commissioner's Office (ICO) after sending a bulk email that identified victims of non-recent child abuse.

The force was at the time investigating allegations of abuse relating to multiple victims. On 19 December 2016, an officer sent an update on the case to 56 recipients by email but entered their email addresses in the 'To' field and did not activate the 'BCC' function, which would have prevented their details from being shared with others.

Each recipient of the e-mail – which potentially included victims, witnesses, lawyers and journalists - could see the full names and e-mail addresses of all the others. The email also made reference to schools and other organisations being investigated in relation to the abuse allegations.

Of the 56 emails sent, all but one was considered deliverable. Three were confirmed to have been successfully recalled once the force identified the breach two days later, so 56 names and email addresses were visible to up to 52 recipients.

# Bayswater Medical Centre

Bayswater Medical Centre in London has been fined £35,000 by the Information Commissioner's Office after it left highly sensitive medical information in an empty building.

The personal data, which included medical records, prescriptions and patient-identifiable medicine, was left unsecured in the building for more than 18 months.

## Nuisance calls?

Nuisance marketing calls are unwanted phone calls that attempt to promote a product, service, aim or ideal to you. For example a caller could try to sell you something or ask you to support a particular cause.

There are two types of marketing calls:
Live marketing calls: unwanted marketing calls from a real person.
Automated marketing calls: pre-recorded marketing messages that are played when you answer the phone.

**What can I do to avoid nuisance live marketing calls?**
To help stop nuisance live marketing calls you can:
register with the TPS free of charge (you can register mobile numbers as well as landlines). The TPS is a central register of individuals who have opted out of receiving live marketing calls.
Check privacy statements when you provide your phone number; and tell organisations you deal with if you don't want them to market you by phone.
Please note, if you agreed that a particular organisation could make live marketing calls to you but you then subsequently registered your number with the TPS, your initial consent to that organisation still remains. You can of course withdraw your consent to marketing calls however you will need to contact the organisation directly to do this.

**What can I do if I am receiving nuisance automated calls?**
Some calls you receive may ask you to phone a premium rate number. The Phone-paid Services Authority (PSA) regulates products or services that are charged to users' phone bills or pre-pay accounts. You can contact them to report these calls or to access details of the premium rate number ranges the PSA regulates.

**Silent or abandoned calls**
These are calls when you answer the phone and there's no one there.
If you are receiving silent calls, you can get more advice from Ofcom on 020 7981 3040.

## A former head teacher fined for illegally obtaining personal data

A former head teacher who obtained personal information about schoolchildren has been prosecuted. The information included names, unique pupil numbers, pupil attainment and progress spreadsheets, along with performance management data for staff.

Darren Harrison, of Twickenham, obtained the information from two primary schools at which he had previously worked and uploaded the data onto his former school's servers. Mr Harrison stated that he took the data from the system for professional purposes.

Mr Harrison appeared before Ealing Magistrates' Court and admitted two offences of unlawfully obtaining personal data, in breach of s55 of the Data Protection Act 1998. He was fined £700, ordered to pay costs of £364.08 and a victim surcharge of £35.

## A former doctor's surgery employee who inappropriately accessed the records of patients and staff members

A former doctor's surgery employee who inappropriately accessed the records of patients and staff members has been prosecuted.

Hannah Pepper, 23, of Syderstone, Norfolk, accessed the electronic clinical records of 228 patients and 3 staff members outside of her role as an administration assistant.

Pepper appeared before King's Lynn Magistrates' Court and admitted 4 offences of unlawfully obtaining personal data, in breach of s55 of the Data Protection Act 1998. She was fined £350, ordered to pay costs of £643.75 and a victim surcharge of £35.

## Inappropriately accessing medical records

It was recently reported in the press that the electronic medical record of former Manchester United Manager Sir Alex Ferguson had been accessed by a number of staff at the hospital where he was treated for a serious illness. An audit showed that a number of staff identified were not involved in his care as such their access was investigated.

This type of incident is not new. Occasionally for personal gain (selling information to the press) or sometimes just personal curiosity, staff not directly involved, but with system access rights, have been tempted to look at records of famous or newsworthy individuals, and many have been caught doing it.

Modern electronic records maintain security of data with only staff who have legitimate access being allowed to see them. However this level is not all that granular, so all the staff on a ward or in a hospital department for example, or at a GP Practice, may have potential access to a cohort of records but only those who actually need to use the access are entitled to actually look at a specific patients record.

Modern electronic records have excellent audit functions that can show exactly who has looked at records, and when, and these audit trails can provide the evidence needed to take action against staff where necessary.

Actions taken against staff can be significant ranging from internal disciplinary action, sanctions from a professional regulatory body, and even criminal prosecution under data protection law.


## Charities caught out!

**1**. Some charities profile their donors based on their wealth. They hire companies to investigate income, property values, lifestyle, and even a person's friendship circles in order to find the most wealthy and valuable donors. These companies also identify donors they believe charities should target because they are most likely to leave money in their wills – they call this legacy profiling.

**What's wrong with that?**

Donors are oblivious to this practice. If you don't know it's happening, you can't object.

---

**2.** Some charities hire companies to find missing information or update out of date information in their databases. These companies use information that has been provided by the donor to track down new data or fill in the gaps. For example, they may use your old telephone number to find your new one or they may use your email address to track down your postal address.

**What's wrong with that?**

You have a right to choose what personal information you provide and you don't have to update your details with a charity if you don't want to. Charities could use the additional information they uncover, which you do not know they have, to contact you for more money.

---

**3.** It is common for some charities to exchange donor information, through an external organisation, with other charities to get details of prospective donors.

**What's wrong with that?**

You can choose to let charities share your information with other organisations but charities must make it clear who these organisations are – for example an animal charity could ask you to let them share your details with other animal charities or it could name the specific other charities it wants to pass your details to. However some charities don't know who they are sharing your details with.

So, for example, supporters of animal charities could have their information shared with homeless, humanitarian or religious charities even though the supporters only expected their information to be shared with other animal charities. This is not acceptable data sharing. Some charities don't know if the information has been shared one or one hundred times. This can result in lots of unwanted charity marketing.

---

# FOCUS ON: Use of domestic CCTV

There are many domestic CCTV systems on the market to help you protect your home. If you're thinking of using one, you need to make sure you do so in a way that respects other people's privacy.

If you set up your system so it captures only images within the boundary of your private domestic property (including your garden), then the data protection laws will not apply to you.

But what if your system captures images of people outside the boundary of your private domestic property – for example, in neighbours' homes or gardens, shared spaces, or on a public footpath or a street?

Then the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) will apply to you, and you will need to ensure your use of CCTV complies with these laws. This guidance refers to them as the 'data protection laws'.
Regardless of whether or not your use of CCTV falls within the data protection laws, the ICO recommends you use it responsibly to protect the privacy of others.

**What does 'private domestic property' mean?**

It means the boundary of the property (including the garden) where you live. This can include rented property, or a private space in a communal residential dwelling – such as a flat, or a private room in a residential care home.

**How can I use CCTV responsibly at my property?**

You should ask yourself whether CCTV is actually the best way to improve your home security.

Think about the following questions:
Do I really need CCTV?
Are there other things I could use to protect my home, such as better lighting?
What is the most privacy-friendly way to set up the system?
What areas do I want the cameras to capture?
Can I position the cameras to avoid intruding on my neighbours' property or any shared or public spaces?
Do I need to record the images, or is a live feed enough?
Has my CCTV system got an audio-recording facility?

Audio recording is very privacy-intrusive. So in most cases where householders use CCTV, they should disable audio recording.
Think about the problem you are trying to tackle. It will usually be to safeguard you and your property against crime. Check your local police advice about crime prevention. Better locks, security lighting or an alarm system may be more effective and less expensive ways of securing your property.
If you decide to use CCTV, think about what areas need to be covered, and whether your cameras need to capture images beyond the boundary of your property. Remember, if your cameras don't capture images beyond your boundary, the data protection laws won't apply to you.

**What is the law if my CCTV captures images of people outside my own home and garden?**

If your CCTV captures images beyond your property boundary, such as your neighbours' property or public streets and footpaths, then your use of the system is subject to the data protection laws.
This does not mean you are breaking the law. But it does mean that, as the CCTV user, you are a data controller. So you will need to comply with your legal obligations under the data protection laws.
You can still capture images, but you need to show you are doing it in ways that comply with the data protection laws and uphold the rights of the people whose images you are capturing.

**What must I do if I capture images of people outside my own home and garden?**

If you are capturing images beyond your property boundary, you should have a clear and justifiable reason for doing so. In particular, you will need to think why you need these images. If asked by an individual or the ICO, you will need to be able to explain your reasons, so you should write them down now. You should also write down why you think capturing the images is more important than invading the privacy of your neighbours and passers-by.

**You will also need to**:

Let people know you are using CCTV by putting up signs saying that recording is taking place, and why.
Ensure you don't capture more footage than you need to achieve your purpose in using the system.
Ensure the security of the footage you capture – in other words, holding it securely and making sure nobody can watch it without good reason.
Only keep the footage for as long as you need it – delete it regularly, and when it is no longer needed.
Ensure the CCTV system is only operated in ways you intend and can't be misused for other reasons. Anyone you share your property with, such as family members who could use the equipment, needs to know the importance of not misusing it.


## Creating Strong Passwords…

Yes, we know strong passwords are important. But the password-cracking capabilities of a hacker are considerable. A hacker would always test common 'weak' passwords (e.g. password123; admin; 123456 etc.), but would certainly also use lists of hacked username/passwords, as well as packet sniffing to seek encrypted authentication requests, which they can then run through a list of known encrypted passwords (containing 10 billion+ passwords).

So here is a simple way to create (and remember) strong passwords:
Firstly, we know a strong password:
Contains 12 characters (minimum)
SHOULD NOT contain dictionary words (or a combination of)
Should have a mixture of upper and lower case letters
And include numbers and special characters, e.g. !£$^*@

1. Start with a memorable song, phrase, or quote:
As an example, we'll use: "Life has no limitations, except the ones you make"
2. Take the first letter from each word and alternate upper and lower case letters:
LhNlEtOyM
3. Add memorable numbers - your year of birth - in reverse:
LhNlEtOyM7791
4. Add special characters and make the password (semi) unique, for use with different accounts:
LhNlEtOyM7791@AZ (for Amazon) LhNlEtOyM7791@EB (for eBay)

So there you go – very strong passwords which you can easily remember! A further advantage being that they can be updated if needed by just changing a single number in the year.

## Clear Desk Policy

At the end of the working day or when leaving the office during the day, all documents should be secured in lockable office furniture.

Removable media shall be locked away and personal belongings should be removed from view.

Office/work area windows shall be closed when working areas are unattended and at the end of the working day.

All internal doors shall be closed when working areas are unattended and at the end of the working day.

In ground floor work areas, blinds shall be closed or PC/Laptop screens, information boards or any protectively marked or sensitive information shall be positioned so it cannot be viewed by passers-by.

All desk pedestals shall be locked when working areas are unattended and at the end of the working day.

All cabinets shall be locked when working areas are unattended and at the end of the working day.

All laptops shall be secured in suitable containers when working areas are unattended and at the end of the working day.

All printers shall be cleared of printed material when working areas are unattended and at the end of the working day.

All photocopiers shall be cleared of printed material when working areas are unattended and at the end of the working day.

All ‘white boards’ shall be wiped clean when working areas are unattended and at the end of the working day.

All ‘flip charts’ shall be cleared of information when working areas are unattended and at the end of the working day.

# Phishing

**Scam watch: TV Licence phishing scam leaves victims £200,000 out of pocket**

Fraudsters are sending out fake TV Licensing emails to steal personal and financial information in order to trick people into parting with their cash.
Action Fraud, the UK's anti-fraud agency, has issued the warning after receiving thousands of reports on fake TV Licensing emails.
In December 2018 alone, Action Fraud received 200 crime reports in relation to TV Licensing emails, with victims reporting a total loss of £233,455.
It says the new wave of TV Licence phishing emails are part of larger fraud, in which criminals are calling victims and claiming to be bank employees.

**How the scam works**

Fraudsters are sending out fake TV Licence emails regarding refunds and payment issues.
The emails use headlines such as 'correct your licensing information', 'billing information updates' and 'renew now' to trick people into clicking on the link within the email.
After a week or two, the fraudster then phones the victim claiming to be from the fraud department of the victim's bank.
They manage to convince victims they are genuine banking staff by using the personal details that the victim provided through the fake website.

The fraudsters then claim that the victim's account has been compromised, possibly by a phishing scam they may have fallen victim to recently, and that they need to transfer their money to a new 'safe account'.
Pauline Smith, director of Action Fraud, says: "Bank staff and police officers will never ask you to move money to a safe account.
"It is also important that you never click on links in emails you were not expecting.
"TV Licensing will never email customers, unprompted, to ask for bank details, personal information or tell you that you may be entitled to a refund.

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site.

**How to protect yourself**

An organisation will never email you unprompted, to tell you that you're entitled to a refund or ask for bank details or personal information.

Don't assume a phone call or email is authentic. Just because someone knows your basic details (such as your name or address), it doesn't mean they are genuine. Criminals can easily spoof the phone numbers and email addresses of companies you know and trust.

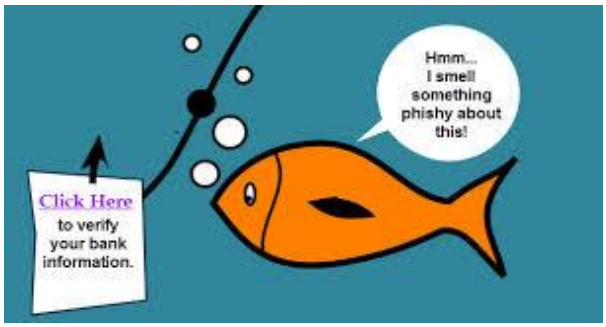
Always question unsolicited requests for your personal or financial information, and never click on the links and attachments in emails or texts you receive out of the blue.

Your bank will never call and ask you for your PIN, full banking password, or ask you to transfer money out of your account.

**What to do if you've fallen victim**

Let your bank know as soon as possible and monitor your bank statements regularly for any unusual activity.
If you suspect your identity may have been stolen you can check your credit file quickly and easily online.

You should do this every few months anyway using a reputable service provider and following up on any unexpected or suspicious results.



## Help and guidance

The eMBED IG Team are here to help and support you in all matters relating to confidentiality, information governance and information security.

**How *can we help you?***

**Our Information Governance Team provides advice and assistance with:**

- The General Data Protection Regulation (GDPR)
- Data Protection Act
- Caldicott Guidelines
- Information Assets
- Data Flows
- Data Protection Impact Assessments (DPIA)
- Creation and delivery of bespoke staff training and awareness sessions
- Information sharing protocols and agreements
- Data processing contracts
- Breach reporting
- Patient and staff confidentiality
- Lasting Power of Attorney
- Support developing policies and procedures related to Information Governance and Data Security

## Key eMBED IG Contacts

**IG Helpdesk:** *eMBED.infogov@nhs.net*

**Information Governance:**
Information Governance Team Manager
*Caroline Million - email: caroline.million@nhs.net*

**Information Security & RA Team Manager:**
*Barry Jackson – email: barry.jackson@nhs.net*

**IG Lead contacts for CCG:**

- Airedale, Wharfedale and Craven, Bradford City and Bradford Districts

*Suzanne Sugden - email: suzanne.sugden@nhs.net*
currently being covered by Jonathan Mayes – email *Mayes.Jonathan@nhs.net*

- Rotherham and Bassetlaw

*Claire McInnes - email: clairemcinnes@nhs.net*

- Sheffield and Barnsley

*Gershon Nubour - email: gershon.nubour@nhs.net*

- East Riding and Vale of York

*Hayley Gillingwater- email:* hayley.gillingwater@nhs.net

- Harrogate & rural, Hambleton, Richmondshire & Whitby, Scarborough & Ryedale

*Helen Sanderson - email:helensanderson@nhs.net*

- Hull, North East Lincs and North Lincs

*Mark Culling - email: mark.culling@nhs.net*

**Primary Care Specialist:**
*Helen Thomis - email: embed.infogov@nhs.net*

## IG Portal

**The IG portal is an invaluable tool aimed at both CCG's and GP Practices and contains template documents for toolkit compliance, an informative Blog, as well as a huge array of general IG information and links.**

**Come visit us at:**

https://portal.yhcs.org.uk/web/information-governance-portal/home