

Guidelines for Safe Disposal of Electronic Yellow Card Data for External Users

1. Scope

This guideline provides a brief on general procedures for the safe disposal of externally held paper and electronic¹ Yellow Card data for applicants requesting access to Yellow Card data for scientific research.

2. Introduction

The MHRA and most other modern organisations are increasingly dependent on computer systems. Substantial costs may be incurred if a system, or the information it contains, is lost, damaged, destroyed or if information is obtained by those not entitled to it. Large amounts of valuable information can be easily stored on external computers and portable computing devices, such as laptops, notebooks, smart phones and Personal Digital Assistants (PDA). It is therefore paramount to ensure data is protected by both minimising the amount of information stored and adequately safeguarding it.

The Data Protection Act 1998 (DPA) applies to personal data. Its purpose is to ensure that such data are processed fairly and lawfully and in particular that personal data is not disclosed to third parties unlawfully. The DPA covers computer records, discs, CDs, USB memory sticks and information held in paper files (e.g. index cards, filing systems etc).

The seventh data protection principle requires data controllers to ensure that appropriate security measures are in place to prevent the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. When the processing of personal data is carried out by a data processor on behalf of the data controller, the contract for that processing must require the data processor to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

Whether the measures in place are appropriate will depend upon whether they provide a level of security appropriate to the harm which might result from a breach of security and the nature of the data to be protected, taking into account the state of technological development and the cost of implementing the measures.

3. Background

The MHRA operates post-marketing surveillance systems for reporting, investigating and monitoring adverse reactions to medicines and adverse incidents involving medical devices to safeguard public health. The safety of medicines is monitored using the Yellow Card Scheme which has been in existence since 1964.

The Independent Scientific Advisory Committee for MHRA database research (ISAC) and the MHRA consider that confidentiality of Yellow Card data is paramount. For this reason such data is provided to third parties on the following stringent conditions.

4. Data Use

4.1 Desktop Computers

If you use a desktop Personal Computer (PC) you must:

¹ Data/Bits & bytes, stored on a digital storage device, e.g. hard disk, flash memory key, CD-ROM etc

- Have adequate security in place at all times when you are not using it, i.e. lock the office when no one is there;
- Ensure that your computer receives regular Operating System security patches, firewall and anti-virus updates;
- Be familiar with your computer's connection capabilities. If it has network/telephone access, be sure to know how you can securely connect to an authorised network or the Internet. Be sure to disconnect any network/telephone connections and to turn it off when not in use;
- You must understand the level of data you are using. Never store or process information with protective markings unless authorised to do so and in a secure environment;
- Be aware of your surroundings and of the opportunity for un-authorised people looking 'over your shoulder.'

The items above are not exhaustive and provide general pointers to make you aware of the types of issues involved. It is always important to 'err, on the side of caution'.

4.2 Portable computers

Due to risk of theft, portable computers (including PDAs, laptops etc) must not be used to store identifiable Yellow Card data. Data must be stored at all times in the location you have told the MHRA.

4.3 Encrypting data for transmission

Recipients of Yellow Card data can only send data to third parties with permission of the MHRA, for example if an applicant has obtained data through an ISAC application and these data need to be shared electronically with a co-applicant.

Many software applications² are available that can encrypt files (of any size) to increase protection against unauthorised disclosure. These files can then be copied onto removable storage media (such as CD) for safer transportation and can also be sent as attachments via standard email. The current (2006) US government approved encryption standard (and adopted in the UK) is the 'Rijndael - Advanced Encryption Standard' (AES).

AES is currently the most secure encryption standard available and is recommended for the encryption of identifiable Yellow Card data, if for any reason a researcher needs to send identifiable Yellow Card data by email to another colleague.

4.4 How to comply with the Advanced Encryption Standard when encrypting Yellow Card data for transportation

If sending data as outlined in 4.3, a few options are available:

4.4.1 Winzip

WinZip(v10) can encrypt data using the approved AES encryption algorithm. The European Medicines Agency (EMA) has selected this method for the safe dispatch of information to its delegates and other Agencies.

4.4.2 Secure Email delivery Service

² Dedicated 3rd party specialist applications are available. Also many leading compression applications have the facility to encrypt (& compress) data e.g. WinZip (v9 & above) or WinRar.(v3.6 & above)

Another method is the use of a secure email delivery service. Encrypting an entire email message (including attachments) prevents 'outsiders' from reading it when it is in transit. There are two options:

1. Configure an email client (e.g. Outlook) to digitally encrypt and sign documents prior to transmission. This method requires the recipient's email application to be configured to successfully accept and decode the encrypted email.
2. The use of a secure web-based email delivery service, such as the popular Hushmail (hushmail.com) or Voltage mail (vsn.voltage.com/index.htm). The registered user would build the message on-line via the web interface and add any attachments before sending the email to the recipient. The recipient would not have to be a registered user to receive the email. However, he/she would have to register to send encrypted email via the service.

5. Data Removal Guidelines

You must be cautious of the fact that in the event your computer is sold or stolen, the data can potentially be accessed by unscrupulous people.

It is a professional and moral obligation to protect (in accordance with the DPA) sensitive Yellow Card data which is no longer required, from unnecessary disclosure. When required, data stored on a computer must be carefully disposed of in an efficient and cost-effective manner. The data owner must be certain that Yellow Card data which is no longer required is obliterated.

Proper organisation of research data on large storage devices is important as this will allow you to safely locate and clear the data, minimising the risk of accidental erasure. Ideally, Yellow Card data should be stored under a main folder. In order to manage large amounts of data, other folders should be created, these folders should be created in a hierarchy structure. This will make the task of shredding individual or even large chunks of data files easier and safer.

6. Hard Disk File Shredding

Proper organisation of research data on large storage devices is important as this will allow you to safely locate and clear the data, minimising the risk of accidental erasure. Ideally, research data should be stored under a main folder. In order to manage large amounts of data, other folders should be created, these folders should be created in a hierarchy structure. This will make the task of shredding individual or even large chunks of data files easier and safer.

6.1 Removal Methods for NHS/DH

The NHS/DH computer system is part of a secure 'restricted' network (this is the minimum classification level for the NHS), so Yellow Card data stored on NHS computers can be deleted in the normal way, in accordance with the organisation's IT policies. The NHS routinely adopts special procedures when computers need to be removed for disposal or a hard disk upgrade is required. If machines are reused internally they are simply rebuilt/re-imaged, if they are leaving the NHS then they are completely wiped clean using an accredited software application or degaussed for extra security. This echoes the Department of Health's (DH's) policy for erasing/discarding computers.

6.2 Removal Methods for non-NHS/DH organisations

6.2.1 Best Practice

When handling sensitive data, the following recommended options provide a safer and more secure data disposal environment.

The 'best practice' method would be a combination approach which includes:

- The creation of a formal computer data disposal document (like this one) explaining the process.
- The use of data wiping software or 'File Shredding' software
 - Where the user does not have a separate drive solely for working with Yellow Card data, File Shredding is the recommended option. File shredding is a technique used to wipe individual folders or files residing on hard disks but can also be used on other removable read/write media. The software will typically run a routine that deletes the chosen files/folders and then overwrites the areas of the hard drive with repeated patterns of random characters. The more "passes" made by the overwriting routine, the harder it becomes to recover the original information.

Recommended File Shredding software is Blancco's File Shredder³

- Where the user has a separate drive letter (i.e. another partition) allocated for working with Yellow Card data, an option is to 'wipe' that drive partition using the recommended software. The partition will be completely wiped, overwritten many times (US Dept of Defence (DoD) standard) and may require the standard re-formatting. This method is ideal and will satisfy all critical concerns about possible recovery of sensitive data. However, this option requires additional technical knowledge.

Recommended software - the Government's, Communications Electronic Security Group(CESG) approved: *OnTrack's 'Data Erasure v2' Pro OR the Blancco Pro application.*⁴

- Use of data encryption software to maintain good security in the event the PC equipment is stolen and/or any unauthorised recovery of deleted data is performed
 - The whole system can be easily and transparently encrypted. Usually one additional password is required at boot up (to allow access) and the system can be used normally

Recommended Encryption software - Bcrypt Disk Protect⁵

6.2.2. Hard Disk Disposal/Re-use

When disposing hard disks containing Yellow Card data the MHRA recommends

- **The government (CESG) approved *OnTrack's 'Data Erasure v2' Pro OR the Blancco PRO application*⁶.**

Please note that when wiping Yellow Card data from your storage media, the software must comply with the 'Gutmann' and US DoD. Of these, the Gutmann standard is most secure – use for personalised/identifiable medical data or documents classified as 'Confidential' or above, for other cases the US DoD

³ Blancco - <http://www.blancco.com/main.site?action=siteupdate/view&id=21>

⁴ OnTrack - <http://www.ontrack.co.uk/dataeraser/>

⁵ Bcrypt Disk Protect - http://www.bcrypt.com/our_products/disk_protect.php

⁶ Data Eraser - <http://www.ontrack.co.uk/dataeraser/>

standard is suitable. If you wish to use a different software package please contact the MHRA to see if it is suitable.

Be sure to understand all the places where data duplication may be located. Data residing on removable storage media (including for backup purposes) such as, CD/DVD's, USB Flash memory devices, floppy disks etc. need to be completely erased using the appropriate disk wiping software. If appropriate, the medium should be destroyed by physically breaking or shredding, this procedure is also known as purging.

6.2.3. Physical destruction/purging

Shredding

This is the most popular method of destroying paper or even CDs and floppy disks, etc. Shredders preferably the 'cross-cut' variety, come in a variety of sizes and capacities for office environments. For larger volumes, hiring the services of specialist vendors for disposal of information may be required. Some vendors will bring equipment to your facility and shred documents on site. If records are to be shredded on the vendor's premises, certified shredding is required.

Purging

Whilst shredding works for paper and CDs, disposal of stronger rigid materials such as hard disks, digital tapes or optical disks require degaussing, pulverisation, drilling, melting/incineration (tasks usually outsourced). Sanding off the physical recording surface is another option.

MHRA/IMD

November 2006