**London Community Equipment Consortium**

**Community Equipment Services – NRS Cyber Attack**

**Frequently Asked Questions for Residents**

**Issue 1 – 15 May 2024**

**1.           What happened?**

Our community equipment services provider, NRS Healthcare, experienced a cyber-attack in late March/early April 2024. We have been having twice weekly meetings with NRS since that time. We have, to date, been informed that no personal data for any user of the service, such as you, had been identified.

In the past week or so however, we have been told that there may be a significant risk that individual service user’s personal data may have been taken and may be published.

We understand this may be concerning for you and NRS is working hard to get details as soon as possible to identify if your data was compromised or not. If we find that it has been, you will be contacted directly.

**2.         What is the Council and NRS Healthcare done to manage the situation?**

On identifying the issue in late March/early April 2024, NRS immediately shut down their systems, and implemented their business continuity plan including appointing external specialists to help understand the extent of the issue.  NRS notified the Council of the incident, NRS also informed the Information Commissioner’s Office (ICO) which oversees the safeguarding of information rights and the Police who are undertaking a criminal investigation. The Council’s Officers also reported to the ICO and Senior Management Teams within the Council.

**3.           How could this happen?**

The number and intensity of these cyber security incidents are increasing, affecting many organisations including those in the healthcare sector. The Council has been working closely with NRS to ensure we have up to date information on the level of risk to you as a service user.

**4.         What is the current position?**

NRS have been working to resolve matters and restore the service as swiftly as possible. The ongoing investigation has now identified that a number of files were stolen in the attack that are likely to contain personal data relating to our residents. We are still unclear whether your information was amongst those data taken. if it is likely that your data has been compromised, you will be contacted directly. In the meantime, we are here to provide advice and guidance.

**5.          What should I do to check if I have been a victim of fraud?**

The following courses of action are recommended:

1. Inform your bank, building society and credit card company of any unusual transactions on your statements.
2. Request a copy of your credit file for any suspicious credit applications. Organisations such as Experian ([www.experian.co.uk](http://www.experian.co.uk)) and Clear Score ([www.clearscore.com](http://www.clearscore.com) ) provide free credit reports.
3. Report the incident to Action Fraud on 0300 123 2040 or you can use their online incident reporting or find additional help and support at [www.actionfraud.police.uk](http://www.actionfraud.police.uk)
4. If you need more help, contact Citizens Advice helpline on 0808 22301133 or via their website: [www.citizensadvice.org.uk](http://www.citizensadvice.org.uk)

**6. Other Useful Information**

Here is some other useful information from the National Cyber Security Centre (NCSC) if you receive any of the following and how to report it to them:

1. If you receive a suspicious text message, forward the message to 7726. This will allow your provider to track the origin of the text message and arrange to block or ban the sender if it is a scam. You can also report scam textmessages to [report@phishing.gov.uk](mailto:report@phishing.gov.uk) and remember to provide a screenshot of your message.
2. Email scams, you can report any suspicious emails to [report@phishing.gov.uk](mailto:report@phishing.gov.uk) Please remember not to click on any of the links within the emails nor open any attachments.

**7. Why are NRS contacting me?**

You will have been recently assessed by a clinician either at hospital or by Adult Social Care at your home and they have recommended some pieces of equipment to support you. The clinician should have explained to you or a family member the process that they use to order equipment for you and when you should be expecting NRS to visit you. NRS will contact you once they have received the order from the clinician to arrange a suitable time to visit you. Once an appointment has been agreed, NRS will send you a text message to advise you on the estimated time of arrival for the Technician.

**NRS will never ask you to provide payment details. If you are asked for any sort of payment, then it is a fraudulent activity. Do not provide any financial information.**

**8. How do I contact NRS Healthcare?**

If you need an urgent repair or require a collection of your equipment, please contact NRS Customer Services on 0300 100 0253 and then follow the menu of options or email[enquiries@london.nrs-uk.net](mailto:enquiries@london.nrs-uk.net)Once an appointment has been agreed, NRS will send you a text message to advise you on the estimated time of arrival for the Technician.

**9.         How will I recognise NRS Healthcare if they attend my home?**

All NRS staff must wear NRS uniforms and carry identification badges, which they must show you before entering. All NRS vehicles are liveried, please see the example below:

**A row of white vans

Description automatically generated**

**10. Key Safes**

If you have a key safe installed, it is advisable to change your key safe code regularly. Instructions have been included in the attached PDF manufacturers user guide.



Alternatively, you can contact the Key Safe Company for help and support through any of the following ways:

* Contact the Key Safe company call centre on 0330 363 0303. The call centre is open Monday – Friday 9am to 5pm.
* Email: [hello@keysafe.co.uk](mailto:hello@keysafe.co.uk)
* Live chat facility at www.keysafe.co.uk

**11. If you require any further advice about this issue?**

Please contact Tower Hamlets Connect by calling 0300 303 6070 or by emailing [enquiry@towerhamletsconnect.org](mailto:enquiry@towerhamletsconnect.org)