Determination and Order

Controller: First Contact Health

Background to the determination

1. On 21 May 2024, First Contact Health became aware of a personal data breach following the compromise of an employee's email account ("the compromised account"), resulting in attempts being made by a threat actor to commit fraud against First Contact Health.

2. On 23 May 2024, First Contact Health notified the Data Protection Authority ("the Authority") of the breach under section 42 of the Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law"). Following a review of information provided by First Contact Health, the Authority had concerns in respect of the security measures that were in place prior to the breach. This resulted in an Inquiry being initiated by the Authority under section 69 of the Law on 3 July 2024.

Reasons for the determination

Sections 6 and 41 of the Law

3. The data protection principles and a controller's responsibility to comply with those principles are set out in section 6 of the Law.

4. Section 6 stipulates that:

> *"(1) A controller must –*
>
> a. *ensure that the processing of all personal data in relation to which the person is the controller complies with the data protection principles in subsection (2)(a) to (f), and*
>
> *(b) comply with the principle in subsection (2)(g).*
>
> *(2) The data protection principles are –*
>
> *…*
>
> *(f)* ***Integrity and Confidentiality:*** *Personal data must be processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*

5. Furthermore, section 41 relates to "Duty to take reasonable steps to ensure security".

6. Section 41(1) stipulates that:

> *"(1) A controller or processor must take reasonable steps to ensure a level of security appropriate to the personal data."*

7. The Authority is of the view that First Contact Health has failed to comply with the requirements of these provisions by virtue of the below:

8. The compromised account was an e-mail account hosted within Microsoft Exchange Online – which was the platform used by First Contact Health to send and receive e-mails internally and externally. These e-mails included health data relating to First Contact Health patients.

9. When processing personal data, a controller must take reasonable steps to ensure a level of security appropriate to the personal data that is being processed. This includes taking reasonable steps to mitigate the risk of unlawful or unauthorised access to that personal data.

10. The minimum level of access controls provided by Exchange Online consists of a single factor of authentication – an e-mail address and password. While this adds a barrier to reduce the risk of unauthorised access, it does not adequately mitigate risk posed by a threat actor that is in possession of the correct credentials. This may happen for several reasons, including credentials being leaked in data breaches, credentials being obtained during a phishing attack or credentials being guessed following a brute-force attack.

11. To mitigate this risk, there are other tools within the Microsoft software suite that should be configured to increase protection against unauthorised access.

12. One such tool that is recommended by Microsoft is the implementation of multi-factor authentication ("MFA"). MFA requires that at least 2 separate conditions be satisfied in order to allow access, generally comprising at least two different factors of either something you know (e.g. username and password), something you have (e.g. a specific device), or something you are (e.g. biometric data).

13. If a threat actor obtains compromised credentials, they must also be able to satisfy the other applicable factor(s) to successfully authenticate and access an account, significantly reducing the likelihood of unauthorised access.

14. When considering the factors outlined within section 41(3) of the Law, MFA should have been implemented by First Contact Health to ensure a level of security

appropriate to the personal data, especially when considering that First Contact Health processes special category data (health data) as a core activity.

15. While MFA does not necessarily prevent all unauthorised access, Microsoft studies1 in 2022 found that MFA reduced the risk of compromise by 99.22%. To further increase protection, additional measures must also be considered to prevent unauthorised access. These include measures to detect and monitor suspicious authentication activity and to add further access conditions that must be satisfied to allow authentication (e.g. IP address based geo-blocking). Such measures are available to be used within the Microsoft software suite.

16. When considering the factors outlined within section 41(3) of the Law, First Contact Health should have considered the use of measures to detect and monitor suspicious authentication activity and place further controls on authentication activity, to ensure a level of security appropriate to the personal data.

17. First Contact Health indicates that during the implementation of its systems five years ago, it was advised by its then IT provider (the "IT Provider"), that MFA was not a necessary requirement.

18. The use of MFA has been a best practice within industry for several years, with it being widely recommended by software vendors, including Microsoft, by bodies such as the National Cyber Security Centre and by data protection regulators. It is also noted by the Authority that the IT Provider had released a blog post in early 2021 within which it is stated that "The use of multifactor authentication should be enabled wherever possible, web services that don't offer this should be avoided!".

19. Given the prevalence of MFA, including its use within individuals' personal life, it is reasonable to expect that its absence should have been noted, questioned and addressed by First Contact Health.

20. Furthermore, had First Contact Health undertaken a security audit or penetration test in respect of its systems, it is reasonable to expect that these basic authentication weaknesses would likely have been identified and therefore could have been remedied at an earlier point.

21. Breach preparedness is a dynamic rather than static responsibility. Given the ever-evolving landscape of cyber-risks, it is important that organisations not only possess security safeguard tools that are fit for purpose, but establish and follow robust protocols and procedures, and reinforce those tools and protocols through active threat monitoring and security audits.

Conclusion

22. In conclusion:

- First Contact Health did not take reasonable steps to ensure an appropriate level of security for account authentication.
- Measures including MFA, tools to monitor suspicious authentication activity, and tools to add further conditional access requirements to accounts should have been implemented by First Contact Health.
- Had First Contact Health conducted regular security audits or penetration tests, it is reasonable to expect that authentication weaknesses could have been identified and remedied much earlier.
- Had First Contact Health implemented these measures, the risk of unauthorised access to the e-mail account would have been significantly reduced, potentially preventing the account from being compromised.

Enforcement Order

23. When the Authority determines that a controller has breached an operative provision of the Law, it may impose a sanction against that controller as outlined within section 73 of the Law.

24. In this case, First Contact Health failed to implement a very basic security measure to ensure the security of personal data within an e-mail account. This e-mail account was subsequently compromised, allowing a threat actor access to data contained within the account, including medical data.

25. Further, First Contact Health failed to demonstrate robust security safeguard procedures in the form of ongoing threat detection, monitoring and security infrastructure review.

26. Therefore, the Authority has decided to issue an enforcement order requiring that First Contact Health take specific action to comply with sections 6 (*'Integrity and Confidentiality'*) and 41 (*'Duty to take reasonable steps to ensure security'*) of the Law.