HEABC
HEALTH EMPLOYERS ASSOCIATION OF BC

FAQs

July 2023

HEABC Cyber Security Attack and Potential Privacy Breach

On July 13, 2023, HEABC learned that it was a victim of a cyber-attack, and subsequently identified that the information taken may have included personal information. Following are frequently asked questions and answers regarding this incident.

1. **What happened?**
   HEABC experienced a cybersecurity incident. The incident resulted in an unauthorized entity obtaining some information from HEABC systems. HEABC has notified the Office of the Privacy Commissioner of BC, the Canadian Centre for Cyber Security, and the RCMP.

2. **How were hackers able to gain entry to these systems?**
   This is the subject of our ongoing investigation.

3. **Does the privacy breach put any patient medical information at risk?**
   No.

4. **When did you first learn about the incident?**
   HEABC first learned that some personal information was potentially involved in the incident on July 13, 2023.

5. **Whose information was potentially involved in this incident?**
   Individuals whose information was potentially involved may include anyone whose personal information was held by HEABC in relation to Health Match BC, the BC Care Aide and Community Health Worker Registry, and Locums for Rural BC program.

6. **Has this cyber-attack impacted recruitment and other services these programs provide?**
   All existing/returning users of these services continue to have access to their accounts by logging in to their accounts through temporary web pages set up on a clean server after the web server affected by the cyber-attack was taken offline. Services for existing users are not disrupted. Health Match BC and Locums for Rural BC job boards can be accessed by new users by contacting the program to manually set up an account. The public-facing websites remain offline and job boards are not visible to anyone without an account. Public information typically available on websites related to incentives, immigration, employment, and registration is currently unavailable but may be accessed by contacting the program directly.

7. **What has HEABC done to respond to this issue?**
   After learning that some information may have been taken from its systems, HEABC shut down and isolated the affected server and websites, and immediately engaged cybersecurity professionals to assist with an independent investigation of the incident. HEABC set up two new clean servers to host the affected websites and other web applications that were not affected to ensure that they are secure. HEABC is notifying individuals and is offering complimentary credit monitoring and identify theft protection services.

HEABC
HEALTH EMPLOYERS ASSOCIATION OF BC

FAQs

July 2023

8. **Can the public and health professionals have confidence in providing personal information into HEABC systems in the future?**
   HEABC remains committed to taking all reasonable actions to protect the personal information it collects. We are working with cyber security and privacy experts to continue to ensure that our systems are as safe and secure as possible. Cyber-attacks are an unfortunate reality and governments, institutions and businesses at all levels have been victimized.

9. **Can you guarantee that this won't happen again?**
   HEABC is working with cyber security experts to ensure we are continuing to do all we can to ensure our systems are as safe and secure as possible.

10. **Have you reported this matter to authorities?**
    HEABC has notified the Office of the Privacy Commissioner of BC, law enforcement, the Canadian Centre for Cyber Security, and the BC government.

11. **Have the responsible parties been arrested?**
    We have reported the incident to the RCMP. We do not have further information at this time.

12. **Do you know why these programs were targeted?**
    HEABC has no indication that these programs were specifically targeted.

13. **How many people were potentially affected?**
    Investigative work continues and we have yet to determine precisely how many individuals are potentially affected.

14. **How are individuals potentially affected by this incident being notified?**
    Individuals potentially affected by this incident are being notified by email.

15. **When was the information taken from the affected server?**
    The investigation into the incident has revealed through due diligence the information was taken from the affected server between May 9 - July 2, 2023. There is no evidence at this time that information submitted through the affected websites after July 2 may have been taken.

16. **If the information was taken between May 9 - July 2, 2023, why is HEABC only notifying potentially affected individuals now?**
    HEABC identified on July 13, 2023 that data was taken from our system. We acted immediately to shut down the affected server, transfer all contents of the server to a new "clean" server, and began an investigation to understand the data that may have been taken and to identify the individuals whose personal information may have been taken. We concurrently developed a process to notify individuals whose personal information may have been taken and began notifying individuals on August 1, 2023.

17. **Does this incident involve personnel files or employment records?**
    No.

18. **Are all health care employees/workers in BC potentially affected by this cyber-attack?**
    No. Only individuals who created accounts/profiles or submitted personal information through one of the affected websites before June 12, 2023 are potentially impacted. The website databases do not include any employment records/personnel files. The three programs – Health Match BC, BC Care Aide and Community Health Worker Registry and Locums for Rural BC – are not health care employers. They do not hold employment records. In some instances, individuals potentially affected may also be employed as health care workers in BC; however, their employment records/personnel files are not held by these programs, nor are they stored on the affected databases.

19. **Why does HEABC collect personal information?**
    The affected server housed websites used for recruitment, bursary applications and other health systems supports. To provide these services, it is necessary to collect and store some personal information.

20. **Is HEABC providing credit monitoring services?**
    Although HEABC has no evidence of any harm arising from this incident, HEABC is offering services that may include credit monitoring, identity theft insurance, and social media and dark web scanning.

21. **What is HEABC doing to prevent this type of event from happening again?**
    HEABC remains committed to taking actions to protect the personal information it collects. We are working with cyber security and privacy experts to continue to ensure that our systems are as safe and secure as possible. Cyber-attacks are an unfortunate reality and governments, institutions and businesses at all levels have been victimized.

22. **What security measures did/does HEABC have in place?**
    HEABC is unable to disclose details about its IT measures for security reasons.

23. **Was the data that was potentially stolen encrypted / protected?**
    HEABC utilizes a range of measures to protect information and remains committed to taking steps to further enhance its security as part of its ongoing commitment to continually improve security. While some of the information that was potentially involved was encrypted, some of it was not. HEABC is unable to disclose details about its IT measures for security reasons.

24. **Is financial information such as credit card and banking information potentially included in the data that may have been stolen?**
    HEABC does not collect credit card information. A limited amount of banking information is collected by bursary programs, without any associated passwords.

25. **What can individuals do to protect themselves from data/identity?**
    While we have not identified any evidence if misuse of the information potentially involved in this incident, we encourage affected individuals to sign up for the free credit monitoring and identify protection service we have offered, and we recommend that individual remain vigilant, as always, regarding their personal information, including:

- monitor your financial accounts regularly for signs of suspicious activity and contact your financial institution if you have any concerns.
- always use caution when responding to any unsolicited or unexpected communication, particularly those that request personal information or refer you to a webpage that asks for your personal information, even if that communication appears to come from a source that you know and trust.
- change your passwords (such as email) regularly and use unique passwords for each account.
- access additional resources provided by the Canadian Centre for Cyber Security at https://www.getcybersafe.gc.ca/en .
- order a copy of your credit report to monitor for suspicious activity from both Equifax Canada and TransUnion Canada