Cybersecurity Incident FAQs for Health-care Providers that contribute information to BORN Ontario

FOR STAFF WHO MAY ENCOUNTER PATIENTS WITH QUESTIONS ABOUT THE INCIDENT

What happened?
BORN Ontario was impacted by a cybersecurity breach caused by a vulnerability in their data transfer software, Progress MOVEit. The MOVEit vulnerability has affected hundreds of organizations around the world that used the same application to securely transfer their data. BORN Ontario used this application to securely transfer data to authorized partners and to move data internally for analysis purposes. As a result of the MOVEit vulnerability, an unauthorized third party was able to access and copy certain files that were in BORN Ontario's possession. Some of the affected information was collected from our organization/practice.

Where can I refer patients who have questions?
Please refer patients to the BORN Ontario site **www.bornincident.ca** which offers information about the incident and will help them determine if they are impacted. BORN Ontario is leading and coordinating the notification effort that will help ensure affected individuals receive clear, consistent, and safe messaging and are provided efficient options to get more information about this breach.

What is BORN Ontario?
BORN Ontario is a pregnancy and child health registry that has been given permission to collect data from health care practitioners across Ontario who provide fertility, pregnancy, birth, newborn and child health care, pursuant to the authority afforded to BORN Ontario in the *Personal Health Information Protection Act*. BORN Ontario links and analyzes data used by healthcare providers and government to improve care and guide clinical decision making. The results are a better healthcare system providing improved healthcare experiences for you and your children.

If a patient has visited the BORN website and still has questions, what can I suggest?
BORN Ontario set up a call centre to help people understand the information provided on the website and to offer an alternative point of contact. Please advise patients to contact the call centre if they have additional questions.

- **1-833-622-1361**
- Available Monday –Friday 9AM to 5PM Eastern time

How can I help reassure patients?
At this time, there is no evidence that any of the data involved in this incident has been misused for any fraudulent purpose or made publicly available. Even though the personal health information contained in the registry is sensitive, BORN Ontario does not collect any personal financial information or the type of information that would typically be used to steal a person's identity. Patients do not need to take any additional steps. BORN has reported the incident to the Office of the Information and Privacy Commissioner of Ontario and they are reviewing the matter.

BORN does NOT collect:

- Health card version codes, expiry dates, or the 9-digit security number on the back, nor scans of the cards themselves.
- Credit card, banking, or financial information
- Social insurance numbers
- Patient email addresses or passwords

Patients should remain vigilant in protecting their information by monitoring their online accounts, creating, and maintaining strong, unique passwords for their online accounts, and reporting any unusual activity to the police and service providers. BORN Ontario will never ask patients for any sensitive personal information by email, text, or phone.

Has the information that was taken been misused/posted publicly?
At this time, there is no evidence to suggest that any of the data involved in this incident has been misused for any fraudulent purposes or posted publicly. BORN will continue to monitor the dark web for any activity related to this incident. If BORN becomes aware of any future misuse of the information, they will provide an update on the website.

Patients should remain vigilant in protecting their information by monitoring their online accounts, creating, and maintaining strong, unique passwords for their online accounts, and reporting any unusual activity to the police and service providers. BORN Ontario will never ask patients for any sensitive personal information by email, text, or phone.

How can patients find out the specific information about them that was accessed?
Unfortunately, due to the complex nature of the incident, we are not able to provide a personalized breakdown of specific information affected on an individual level. BORN deeply apologizes for this incident. For more information on the types of data affected based on the type of care received, patients should refer to the "Am I Impacted?" tab on the incident website (bornincident.ca).
Please advise patients to contact the call centre if they have additional questions.

- ***1-833-622-1361***
- *Available Monday –Friday 9 AM to 5PM Eastern time*

Why aren't patients receiving a letter in the mail or a phone call to notify them that they are affected by this privacy breach?
Because of the sensitive nature of the information and the complexity associated with the breach and the impacted data types, direct notification by phone or mail was not feasible or advisable.

BORN is leading and coordinating a notification effort that will help ensure affected individuals receive clear, consistent, and safe messaging and are provided efficient options to get more information about this breach.

There is no evidence that the information copied in this breach has been misused for any fraudulent purpose or made public. BORN Ontario is maintaining the privacy and identity of those impacted and is not creating any written material that links people to their history of fertility treatment, childbirth, or pregnancy. The incident website offers information to notify patients of the incident and help them determine if they were impacted.

Why is BORN coordinating the notification process?
The cybersecurity incident affected BORN Ontario's records and systems. Our organization's systems were not affected by the cybersecurity breach.

BORN is leading and coordinating a notification effort that will help ensure affected individuals receive clear, consistent, and safe messaging and are provided efficient options to get more information about this breach.

In addition, the complexity associated with this breach and the impacted data types makes direct notification neither feasible nor advisable.