

Frequently Asked Questions About the BCBSMA Data Breach

December 15, 2009

BCBSA PROVIDER DATA INCIDENT

A provider data breach that occurred at the Blue Cross Blue Shield Association in Chicago affected Blue Cross plans across the country. Following are answers to questions the media or other external stakeholders may have.

QUESTIONS AND ANSWERS

1. I heard there was a recent breach of data – what happened?

An employee at the Chicago-based Blue Cross and Blue Shield Association transferred unencrypted provider data to a personal, non-BCBSA laptop. The employee's purpose in doing this was to complete work-related data analyses. However, storing the data in this manner was unauthorized by BCBSA and violated BCBSA's established data security policies. Subsequently, the employee's laptop containing the data was stolen. This theft did not occur on BCBSA premises.

2. What type of data was it?

It included provider personal information, including provider name, address, provider tax number, national provider identification number and social security number.

3. Has the stolen data been used improperly?

There has been no evidence that the data has been used improperly. It appears the target of the theft was the laptop, not the data. However, as a precaution, BCBSA is offering a credit monitoring service.

4. Did the BCBSA employee involved face disciplinary action?

Yes. We have learned that the BCBSA employee faced disciplinary action, which for this type of violation can include discharge.

5. Did the data include information about patients?

No patient Protected Health Information (PHI) was involved in this incident.

6. Was there any PHI included in the data?

No.

7. When did this happen?

The theft occurred August 25, 2009.

8. Why weren't doctors notified sooner?

We apologize for the lapse in time between the incident and the notification. It took some time for BCBSA to set up the Experian credit monitoring service and to share the details with local Blue plans. We also had to ascertain which of our providers had Social Security numbers included in the data file.

9. Why does BCBSA have information about Michigan doctors?

As part of our national BlueCard program, the Blue Cross and Blue Shield Association maintains a database of Blue plan providers so that members may obtain health care services while traveling or living in another service area. In light of this incident, we are reviewing our policies and procedures for sharing data with BCBSA.

10. How will BCBSA prevent this from happening again?

BCBSA employees receive annual and departmental training on privacy and security procedures, which includes using encryption software when saving protected health information and personally identifiable information to mobile devices, and only saving such information to BCBSA-issued devices.

The Association also recently completed updating its PHI/PII inventory and is now reviewing access privileges company-wide to ensure that only individuals with a specific need to have access to applications or files with PHI/PII have such access. Encryption capabilities and requirements are also being enhanced. The Association has purchased new encryption software that automatically encrypts any data copied to mobile media. This software is being deployed to all desktops and laptops. The Association's Executive Privacy and Security Steering Committee will be considering additional controls and evaluating their potential impact to business operations over the next few months.

11. What controls do BCBSM and BCN have in place to ensure this doesn't happen in Michigan?

BCBSM and BCN take our responsibility to protect our stakeholders' information very seriously. We are reviewing our policies and procedures for sharing data with BCBSA. The Blues implemented controls in 2007 and 2008 to automatically encrypt confidential data when downloaded to BCBSM- and BCN-issued laptops and other mobile devices. The company also recently updated vendor contracts to mandate specific security controls to prevent and mitigate the risk of an incident like this. We know stakeholders entrust us to protect their information, and we're committed to preventing these types of situations from occurring again.

12. How have you communicated about this incident?

We have sent a personal letter to every provider who was affected. We have notified the state medical associations. We have provided information to our employees who interact with providers.

13. Why is there only a \$25,000 protection amount for the doctors and the practice?

The \$25,000 insurance amount is to cover expenses that they might need to make in order to resolve any credit issues (items like copies, stamps, calls, coordination, etc.). Detailed questions about fraudulent credit or financial activity should be addressed to the financial institution that opened and/or services the account and Experian.

14. Are you or the Association releasing the name of the employee responsible for this incident?

We are unable to release this information as it could compromise the privacy and safety of the Association's former employee. Providers' attorneys can follow established legal procedures to obtain this information if it is required for any further action they may decide to take.

15. Why were Social Security numbers (SSN) sent to the Association when providers have a Tax ID (EIN) / NPI number?

As part of the BCBSM provider enrollment process, all providers are required to supply BCBSM with their SSN so we can perform our credentialing process. We maintain this number in individual provider records on our systems. The Association requires us to provide them with a weekly individual provider data file, which for BCBSM includes the SSN information stored in individual provider records. In light of this incident, we are reviewing our processes and policies for sharing data with the Association.