

RANSOMWARE INCIDENT RESPONSE WORKSHEET

Use this form in addition to the *Breach/Incident Investigation Report* form in the *Forms* section of the Manual or on the TMC Client Portal. Work with your IT/Security Officer to answer the questions below.

1. Who discovered the attack? _____
 2. How was the attack discovered? _____
 3. What was the date and time the attack was discovered? _____
 4. Which computer/device was the attack discovered on? _____
-

5. Was the PHI restored/recovered? Yes No
If No, was the PHI stolen or removed from the network?
 Yes No Under Investigation (update this answer as needed)

6. Was the PHI encrypted *before* the attack? Yes No

*Risk Point: if the answer is “Yes” the risk of compromise under the HIPAA 4-Part Breach Risk Assessment might be lower.

*Risk Point: the risk of compromise under the HIPAA 4-Part Breach Risk Assessment may be lower depending on the data elements involved in the attack.

7. Was the attack reported to the FBI? Yes No

If “Yes” list the name and contact information of the FBI contact: _____

8. Is the identity of the attacker known? Yes No

If “Yes” list here: _____

9. Was the requested ransom paid to the attacker? Yes No

RECOVERY DETAILS

1. What systems/databases and machines were impacted by the attack? If unknown, return and update this answer as needed. _____

2. Were there any back-ups available to be restored? Yes No
 - If “No” were the back-ups corrupted? Yes No
 - If “No” were there no back-ups retained to be restored? Yes No
 - If “No” was a partial back-up used or something else? If so, describe. Yes No

3. If a partial back-up was restored, what is the date of the last backup? (e.g. all but the most recent 2 months have been restored): _____

4. Is there ongoing monitoring for the same or similar virus at least 30 days?
 Yes No
If “No” describe ongoing detection efforts: _____

5. Has malware detection been updated? Yes No

6. Who has been notified of the attack and when:
 U.S. Department of Health and Human Services’ Office of Civil Rights (OCR): _____
 State Attorney General: _____
 Patients: _____
 Other: _____

Include this on your annual risk analysis and retain for 6 years.

Notes/Attachments:
