From the Office of the Inspector General, HHS

Please provide the following:

1. Written narrative describing the breach, including a detailed description of the electronic protected health information (ePHI) involved;
2. Documentation of any internal investigation conducted by (your company) including any police reports;
3. 3. Copy of a forensics analysis report of the incident, if completed, by or on behalf of (your company);
4. Copy of the policies and procedures in place at the time of the breach to safeguard PHI and ePHI;
5. Copy of any enterprise-wide risk analysis prepared by or on behalf of (your company;
6. Any revisions or updates made to the risk analysis to include malware infection or hacking attacks as a risk item;
7. Documentation of the security measures that were put into place to reduce the risk to ePHI identified in the risk analysis (risk management plan), and a description of any updates to the risk management plan with post-breach security improvements;
8. Copy of security awareness and training programs for all workforce members (including management);
9. Copy of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
10. Copy of policies and procedures, or equivalent alternative safeguards, for guarding against, detecting , and reporting malicious software;
11. Evidence of all implemented security measures to reduce the risk to malware infection or hacking, including antivirus software and patching of affected systems) please provide screenshots of relevant computer programs and configuration settings, if applicable);
12. Evidence of network scans or penetration tests performed before or after the incident;
13. Copy of policies and procedures for examining activity in information systems that contain or use ePHI;
14. Policies and procedures regarding workforce members’ access rights. Are these rights reviewed by management?
15. Copy of breach notice to an affected individual and documentation of substitute notice, if applicable;
16. Documentation of the notice provided to the media, the media outlets it was published in, and the dates or duration of publication;
17. Documentation of any corrective action already taken, including revision of policies and procedures, employee training/retraining, additional safeguards, etc.