OCR INVESTIGATION - INITIAL DATA REQUEST

In connection with OCR's investigation into the matters raised by the breach report, we request that *[Business]* provide the following information to OCR within ten (10) business days from receipt of this letter. Please number responses to correspond with the enumerated requests. Electronic copies are encouraged. Please no staples or double-sided pages.

1. The name, title, email address, mailing address, and telephone number of the individual designated to work with OCR during the subject investigation.

2. Please indicate if *[Business]* conducted an internal investigation of the incident. If so, please provide a copy of its finding. Please also provide any corroborating documentation, such as interview notes, police reports, forensic reports, access logs, etc.

3. Please state how many individuals' PHI was disclosed via [breach method]

4. Please provide *[Business]*'s policies and procedures to ensure PHI is safeguarded (45 C.F.R § 164.530(c)), as well as policies and procedures related to impermissible uses and disclosures (45 C.F.R. § 164.502(a)). Indicate the dates of implementation and any redrafting of the policies, since April 14, 2003.

5. Please indicate any and all steps taken to mitigate the potential harm caused by the impermissible disclosure of PHI through [breach method].

6. Please provide *[Business]*'s policy on notifying individuals in the event of a breach of PHI. (45 C.F.R. § 164.404). Please also provide a sample copy of the breach notification letter that was issued to affected patients regarding the incident. Please include the dates of notification. If no notification was sent to individuals, please state so.

7. Please provide evidence that *[Business]* provided notice to a prominent media outlet. The evidence should include documentation that notice was provided without unreasonable delay and within the requirements of 45 C.F.R. § 164.406. If no notification was sent to the media, please state so.

8. Please provide evidence that *[Business]* provided notice to a HHS pursuant to the requirements of C.F.R. § 164.408. If no notification was sent to HHS, please state so.

9. Please submit a copy of *[Business]*'s <u>most recent</u> risk analysis, as well as a copy of **all** risk analyses performed for or by *[Business]* <u>within the past 6 years</u> pursuant to C.F.R. § 164.308(a)(1)(ii)(A). If no risk analysis has been performed, please state so.

10. Please provide evidence of *[Business]*'s security measures that are in place to reduce the risks to ePHI identified in the risk analysis (i.e. risk management plan and accompanying evidence). Please be sure to submit a copy of a risk management plan associated with each risk analysis requested above. These risk management plans should describe the security measures implemented by *[Business]* to sufficiently reduce the risks and vulnerabilities identified in the risk analyses to a reasonable and appropriate level to comply with C.F.R. § 164.308(a)(1)(ii)(B). Please ensure the risk management plan states the dates of implementation and/or estimated

dates of completion for each security measure. Provide evidence of implementation where applicable (i.e. screenshots, business associate agreements, photographs, etc.)

11. Please provide documentation on *[Business]*'s sanctions policies and procedures as well as evidence of any sanctions applied to applicable workforce members pursuant to this incident. (45 C.F.R. § 164.308(a)(1)(ii)(C)).

12. Please provide documentation that system access, audit logs, and incident reports are reviewed regularly. Please also provide policies and procedures regarding reporting and documentation of incidents. (45 C.F.R. § 164.308(a)(1)(ii)(D)).

13. Please provide *[Business]*'s policies and procedures for authorizing access to ePHI systems. Indicate the dates of implementation and any redrafting of the policies, since April 14, 2003. Please also provide evidence that requests for access to ePHI are reviewed and approved by management (45 C.F.R. § 164.308(a)(4)).

14. Please provide evidence that *[Business]* has implemented a security awareness and training program for all members of its workforce (including management). Please be sure to include evidence of security reminders, protection from malicious software, log-in monitoring, and password management. Please also provide *[Business]*'s passwords policy. Indicate the dates of implementation and any redrafting of the policies, since April 14, 2004. (45 C.F.R. § 164.308(a)(5)).

15. Please provide copy of policies and procedures related to security incident procedures. Please include evidence that incident reporting processes are documented, that corrective actions in response to incidents are documented and tracked; and that workforce members are aware of incident reporting processes. (45 C.F.R. § 164.308(a)(6)).

16. Please provide documentation that *[Business]* has procedures in place to report and document suspected or known security incidents; that security incident investigations are conducted in a timely manner; that there are known procedures in place to coordinate security incident investigations with third parties and law enforcement; and that there are processes in place to update and implement policies and procedures based on incident response (45 C.F.R. § 164.308(a)(6)(ii))).

17. Please provide documentation that *[Business]* performs periodic technical and nontechnical evaluations that establish the extent to which *[Business]* security policies and procedures meet the requirements of the Security Rule, as required by 45 C.F.R. § 164.308(a)(8).

18. Please provide *[Business]*'s policies and procedures regarding access rights to ePHI systems, including documentation that *[Business]* periodically reviews and updates employees' access rights. Please include evidence that *[Business]* requires a unique identification and automatic logoff and that it has established an emergency access procedure. (45 C.F.R. § 164.312(a)).

19. Please provide evidence that *[Business]* has a mechanism in place to encrypt and decrypt ePHI; or if no mechanism is in place, evidence of the analysis performed with determined that no such mechanism was required. (45 C.F.R. § 164.312(a)(2)(iv)).

20. Please provide evidence that *[Business]* has in place hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI. Please include documentation that systems that allow access to or store ePHI have logging enabled; that reviews of audit logs occurs regularly; and that workforce members are trained and reminded that their activity is monitored (45 C.F.R. § 164.312(b)).

21. Please provide evidence that *[Business]* has implemented technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network (including evidence of integrity controls and encryption) (45 C.F.R. § 164.312€).

22. Please provide documentation that *[Business]* trains its staff. The HIPAA Privacy Rule requires that covered entities provide training, or proof of training for each new member, or when it makes a material change to its policies and procedures (for example, when a covered entity makes changes to its policies and procedures as part of its corrective action). Training under these circumstances must be completed within a reasonable period of time after the material change becomes effective (45 C.F.R. § 164.530(b)(2)).

23. For OCR's accountability purposes, we are requesting that you provide us with the number of people/patients you serve per day and/or the number of licensed beds you have at your facility. For larger covered entities, OCR is aware that the number of people/patients that you serve per day may be a close approximation. Please also state the total annual budget for the fiscal year.

If you have any questions, please do not hesitate to contact [Investigator].

DATA REQUEST

Please provide a summary of the actions, with any supporting documentation, taken by *[Business]* in response to the breach incident reported to OCR on [date], including:

Privacy Rule:

1. A copy of *[Business]*'s investigation and timeline of the incident
2. A copy of *[Business]*'s HIPAA policies and procedures regarding:
    a. Use and disclosure of protected health information
    b. Safeguards
3. Documentation of all corrective actions taken by *[Business]*, including measures implemented to prevent this type of incident from reoccurring

Security Rule:

1. A copy of the most recent risk analysis performed for or by *[Business]*
2. A copy of the most recent risk assessment performed for or by *[Business]*
3. A copy of the incident report prepared by *[Business]* regarding the breach report, including any corrective actions taken by *[Business]*
4. A copy of policies and procedures regarding review of system access and audit logs
5. A copy of policies and procedures regarding review of incident reports
6. Policy and procedures regarding implementation of periodic technical and nontechnical evaluations, including a copy of the latest evaluation relating to the filtering of case numbers
7. Policies and procedures to protect electronic protected health information from improper alteration or destruction
8. Documentation of security measures taken to reduce risks and vulnerabilities to a reasonable and appropriate level to ensure confidentiality, integrity, and availability of ePHI in *[Business]*'s possession

Breach Notification Rule:

1. Documentation that the affected individuals were notified of the breach
2. A sample copy of the notification to individuals
3. Please state the number of individuals affected in each state/jurisdiction listed in the Breach Report
4. Documentation that substituted notice was provided to individuals as necessary
5. Documentation that the media was notified of the breach
6. A copy of the notification to the media