Cinde Warmington, Esq.
Shaheen & Gordon, P.A.
107 Storrs St.
Concord, NH 03301
(603) 225-7262
cwarmington@shaheengordon.com

November 18, 2009

This decision matrix is provided for educational purposes only and does not constitute legal advice. It is recommended that you consult with legal counsel in the event of a breach. This matrix is intended to explain the interface between HIPAA and NH law with respect to breach notification requirements and thus sets forth only those elements that allow for compliance with both HIPAA and State law. In addition, it does not address the many other issues that arise and that must be addressed when an actual breach occurs.

Assessing the Breach Notification Requirements

1) Determine if the information improperly acquired, accessed, used or disclosed was unsecured PHI?

a) For electronically stored information: Was it encrypted (in accordance with specifications)?

Yes: STOP
No: Go to Q2

b) For PHI in paper/other media: Was it destroyed (in accordance with specifications)?

Yes: STOP
No: Go to Q2

2) Was the information a limited data set with DOB and zip code also removed?

Yes: STOP
No: Go to Q3

3) Does the breach fall into one of the HIPAA exclusions?

a) Unintentional, good faith acquisition, access or use by workforce member or person acting under authority of covered entity within scope of employment and no further use or disclosure in a manner prohibited by HIPAA?

b) Inadvertent disclosure by a person authorized to access PHI to another person at same covered entity or business associate also authorized to access PHI.

c) Disclosure of PHI where covered entity or business associated has good faith belief that unauthorized person would not reasonably have been able to retain it.

Yes: Go to Q4
No: Go to Q6

4) Did the breach include personal information under RSA 359-C:
19 (SS#, Driver's license #, Other Govt ID , Bank Acct #, Credit card #, or Debit card #, in combination with any required access code)?

Yes: Go to Q5
No: STOP

5) Did breach involve good faith acquisition by employee or agent of covered entity or business associate for business purposes with no use or further disclosure?

Yes: STOP
No: Go to Q6

6) Does the breach compromise the security or privacy of the PHI or personal information (pose a significant risk of financial, reputational or other harm to the individual)?
(A determination that misuse of personal information has occurred, is likely to occur or a determination cannot be made would result in a "yes" answer)

Yes: Give notice to Attorney General's Office if personal information included in breach (see content and timeliness requirements under RSA 359-C:20);

Give individual written breach notification; (see content and timeliness requirements); Go to Q7

No: STOP

7) Is there insufficient or out-of-date contact information for written notification of 1-9 individuals?

Yes: Give substitute notice by alternative form of written notice, telephone or other means; Go to Q9
No: Go to Q8

8) Is there insufficient information or out-of-date contact information for written notification of 10 or more individuals?

Yes: Give substitute notice by conspicuous notice posted on web-site or in major print or broadcast media (must include toll-free #); Go to 9
No: Go to Q9

9) Is there possible imminent misuse of unsecured PHI?

Yes: Covered entity may give telephone notice in addition to required notice above; Go to Q10
No: Go to Q10

10) Does breach involve more than 500 residents of a State or jurisdiction?

Yes: Notify prominent media outlets serving State or jurisdiction. Go to Q11.
No: Go to Q11.

11) Does the breach involve 500 or more individuals?

Yes: Notify Secretary of US DHHS at time individuals are notified; Go to Q12
No: Maintain a log and submit to Secretary HHS annually within 60 days after end of calendar year; Go to Q12

12) Does notification involve breach of personal information of more than 1000 individuals?

Yes: Notify all consumer reporting agencies
No: STOP