QUEST, INC
BREACH
NOTIFICATION
POLICY

Dev September 2012

Template HIPAA Breach Notification Policy
Table of Contents

Page Number		
	I.	**Breach Notification**
1	A.	Generally
1	B.	When a Breach is Considered to be "Discovered"
1	C.	Time of Notification
1	D.	Content of Notification
2	E.	Methods of Notification
2	F.	Notification to the Media
3	G.	Notification to the Secretary of HHS
3	H.	Notification from a Business Associate
3	I.	Law Enforcement Delay
	II.	**Administrative Policies**
4	A.	Training
4	B.	Complaints
4	C.	Sanctions
4	D.	Prohibition on Intimidating or Retaliatory Acts
4	E.	Prohibition on Waiver of Rights
5	F.	Changes to Policies and Procedures
5	G.	Documentation
5	H.	Period of Retention
	III.	**Definitions**
6	A.	Breach
6	B.	Compromises the security or privacy of the protected health information
6	C.	Law enforcement official
6	D.	Unsecured protected health information

HIPAA Breach Notification Policy

I. Breach Notification

A. Generally

Following discovery of a breach of unsecured protected health information, Quest, Inc Privacy Officer shall notify each individual whose unsecured protected health information has been, or reasonably believed by the Privacy Officer to have been, accessed, acquired, used, or disclosed as a result of that breach. Such notification shall be as stated in this Breach Notification Policy.

B. Discovered

When a Breach is Considered to be "Discovered."
A breach shall be considered to be "discovered" as of the first day on which the breach is known to Quest, Inc, or, by exercising reasonable diligence would have been known to Quest, Inc. Quest, Inc shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of Quest, Inc.

C. Time of Notification

The notification to affected individuals shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

D. Content of Notification

The notification to affected individuals shall be written in plain language and include to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what Quest, Inc is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

5. Contract procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site, or postal address.

Generally, the notice should avoid including any sensitive material, such as the individual's actual social security number or credit card number.

As appropriate for the individuals to whom notice is given, reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by Quest, Inc and as may be necessary to ensure effective communication with individuals with disabilities.

E. Methods of Notification

1. Written Notice

The notification to affected individuals shall be by first class mail to the individual at the last known address of the individual, or, if the individual has agreed to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

If Quest, Inc knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification may be by first class mail to either the next of kin or the personal representative is permitted. It may be provided in one or more mailings as information is available.

2. Substitute Notice.

a. Generally. If there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice, which is reasonably calculated to reach the individual, must be used. However, substitute notice is not required if the insufficient or out-of-date contact information precludes written notice to the next of kin or personal representative.

b. If Fewer Than 10 Individuals. If there are fewer than 10 individuals to receive substitute notice, the substitute notice may be provided by an alternate form of written notice, telephone, or other means.

c. If 10 or More Individuals. If there are 10 or more individuals to receive substitute notice, then the substitute notice must:

(1) Be in the form of either: (A) a conspicuous posting for a period of 90 days on the home page of the Web site of Quest, Inc; or, (B) a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and,

(2) Include a toll-free telephone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

3. Additional Notice in Urgent Situations

If the Privacy Officer deems the situation to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice stated above.

F. Notification to the Media

If a breach of unsecured protected health information involves more than 500 residents of a State or other jurisdiction, Quest, Inc shall notify prominent media outlets serving that State or jurisdiction of the breach. This notice will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. To the extent possible, the notification shall meet the requirements stated in paragraph I.D, "Content of Notification," above, for its content.

G. Notification to the Secretary of HHS

Following discovery of a breach, the Privacy Officer shall notify the Secretary of HHS as stated below.

1. Breaches involving 500 or more individuals. If the breach involves 500 or more individuals, with one exception, Quest, Inc will provide the Secretary of HHS with notice of the breach contemporaneously with its notice to the affected individuals. The notice will include the same information that is provided to affected individuals and will be provided to the Secretary of HHS in the manner specified on the HHS Web site. The exception is when there is a law enforcement delay (see, paragraph 1.1, below).

2. Breaches involving less than 500 individuals. If the breach involves less than 500 individuals, the Privacy Officer will maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the Secretary of HHS with notice of breaches occurring during the preceding calendar year. (For 2009, the information to be submitted will be only for breaches, if any, occurring on or after September 23, 2009.) This log will be kept for six years.

H. Notification from a Business Associate

When notification is received from a business associate of Quest, Inc of its discovery of a breach of unsecured protected health information, the Privacy Officer shall give notice to affected individuals in accordance with this Breach Notification Policy. Provided, however, if the agreement between Quest, Inc and the business associate permits, the Privacy Officer may require the business associate to give such notice.

I. Law Enforcement Delay

Notwithstanding anything in this Breach Notification Policy to the contrary, if a law enforcement official states to Quest, Inc that a notification, notice, or posting required by this Breach Notification Policy would impede a criminal investigation or cause damage to national security, the Privacy Officer shall:

1. If the statement of the law enforcement official is in writing and specifies how long of a delay is required, delay the notification, notice, or posting for the time period specified in the writing; or,

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily but no longer than 30 days from the date of the statement,

Any member of the workforce of Quest, Inc who is contacted by a law enforcement official in this regard shall immediately refer him/her to the Privacy Officer.

II. Administrative Policies

A. Training

All members of Quest, Inc's workforce shall be trained annually on Quest, Inc's breach notification policy and procedures as necessary and appropriate for the members of the workforce to carry out their functions within Quest, Inc.

Each new member of the workforce shall be trained within (90) calendar days after the person joins the workforce. Each member of the workforce whose functions are affected by a material change in these privacy policies or procedures shall be trained within (30) calendar days after the material change becomes affective.

Documentation of the training for each member of the workforce shall be kept in written or electronic form for six (6) years after the date of its creation or the date that persons ceases to be a member of Quest, Inc's workforce, which is later.

B. Complaints

Quest, Inc's Privacy Officer shall be responsible for receiving complaints concerning Quest, Inc's breach notification policies and procedures and compliance with that policy and those procedures.

C. Corrective Actions

Any member of Quest, Inc's workforce who fails to comply with Quest, Inc's Breach Notification Policy or the requirements of the HIPAA Breach Notification Rule shall be subject to disciplinary review and corrective actions imposed through Quest, Inc's discipline and discharge policies.

Corrections actions which may include termination for those acts which a “Knowing Failure or Violation” occurs. Some but not all types of non compliance which will result in some sort of sanction or disciplinary review follow:

1. Inadvertent failure to promptly report any breach of unsecured private health information to the Privacy Officer.

2. Inadvertent violation of any part of Quest, Inc's Breach Notification Policy or requirement of the HIPAA Breach Notification Rule

3. Knowing failure to promptly report any breach of unsecured private health information to the Privacy Officer

4. Knowing violation of any part of Quest, Inc's Breach Notification Policy or requirement of the HIPAA Breach Notification Rule

D. Prohibition on Intimidating or Retaliatory Acts

Neither Quest, Inc nor any member of Quest, Inc's workforce may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by, this Breach Notification Rule, including filing a complaint under this Rule.

E. Prohibition on Waiver of Rights

No member of Quest, Inc's workforce may require an individual to waive the individual's rights under this Breach Notification Rule as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

F. Changes to Policies and Procedures

The Privacy Officer shall promptly change this Breach Notification Policy as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Breach Notification Rule.

G. Documentation

The Privacy Officer shall take, or cause to be taken, each of the following actions:

1. Maintain Quest, Inc's breach notification policies and procedures in written or electronic form;

2. If a communication is required by Quest, Inc's Breach notification policies and procedures, or by the HIPAA Breach Notification Rule, to be in writing, maintain that writing, or an electronic copy, as documentation;

3. If an action, activity, or designation is required by Quest, Inc's breach notification policies and procedures, or by the HIPAA Breach Notification Rule, to be documented, maintain a written or electronic record of that action, activity or designation.

4. Maintain documentation sufficient to meet Quest, Inc's burden of demonstrating that all notifications were made as required by this Breach Notification Policy or that a use or disclosure did not constitute a breach.

H. Period of Retention

Documentation required by paragraph II.G, "Documentation", above, shall be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

III. Definitions

As used in this Breach Notification Policy, the following terms and phrases shall have the following meanings.

A. Breach

"Breach" means the acquisition, access, use or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. Provided, however, breach does not include:

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of Quest, Inc or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule.

2. Any inadvertent disclosure by a person who is authorized to access protected health information at Quest, Inc or business associate to another person authorized to access protected health information at Quest, Inc or the same business associate, or organized health care arrangement in which Quest, Inc participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

3. A disclosure of protected health information where Quest, Inc or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. Compromises the Security or Privacy of the Protected Health Information

For purposes of the definition of "breach," "compromises the security or privacy of the protected health information" means the breach poses a significant risk of financial, reputational, or other harm to the individual. Provided, however, a use or disclosure of protected health information that does not include the identifiers that must be removed for a limited data set, plus date of birth and zip code does not compromise the security or privacy of the protected health information.

C. Law Enforcement Official

"Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or,

2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law."

D. Unsecured Protected Health Information

"Unsecured protected health information" means protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services (the "Secretary of HHS") through guidance issued by the Secretary of HHS on the HHS Web site.