

GUIDANCE FOR COMPLYING WITH THE HIPAA/HITECH BREACH NOTIFICATION RULE

INTRODUCTION

The American Dental Association developed the following Guidance to help dental practices implement the Breach Notification Rule released on August 24, 2009 by the U.S. Department of Health and Human Services (HHS) entitled *Breach Notification for Unsecured Protected Health Information*. The Rule details whom a HIPAA Covered Entity¹ must notify in the event of a “breach” of a patient’s unsecured protected health information (PHI)—that is, if a patient’s unsecured PHI is acquired, accessed, used, or disclosed in an unauthorized way.

The Guidance addresses breach notification in a user-friendly question-and-answer format and includes the following additional tools to help dental practices understand and prepare to implement breach notification compliance:

- ***Additional Questions and Answers about Breach Notification***
- ***Breach Notification Flow Chart Set***
 - ***Breach Notification Flow Chart***
 - ***Breach Notification Flow Chart Glossary of Terms***
- ***Sample Dental Practice Breach Notification Action List***
- ***Sample Breach Notification Policy and Procedures***
- ***Sample Breach Notification Risk Assessment Worksheet***
- ***Sample Breach Notification Notice to Individual***

Each of these tools provides insight into the Breach Notification Rule in order to help dental practices prepare to comply with the Rule. The effective date of the Rule is **September 23, 2009**. **However, HHS has advised that it does not intend to impose sanctions for breaches that are discovered prior to February 22, 2010.**

¹ A dental practice is a HIPAA “Covered Entity” if it transmits any health information **electronically** in connection with a HIPAA “covered transaction” (such as submitting health care claims to a health plan) or if such information is submitted electronically on the dentist’s behalf. If a dental practice is a HIPAA Covered Entity, HIPAA covers **all** PHI in that practice, whether it is electronic, paper, oral, or in any other form.

Dental practices that are HIPAA Covered Entities must follow the HIPAA Security Rule and the HIPAA Privacy Rule, including the amendments to HIPAA that were enacted under the 2009 Stimulus Act (the “American Recovery and Reinvestment Act,” or “ARRA”) referred to as “HITECH” (the “Health Information Technology for Economic and Clinical Health Act”).

Covered Entity dentists must also follow any applicable **state** privacy or confidentiality laws that are more stringent than HIPAA. Even if a dentist does not meet the definition of a Covered Entity under HIPAA, state privacy and confidentiality rules apply to the practice.

While this Guidance attempts to provide dentists with information needed to comply with the federal Breach Notification Rule, the Guidance and accompanying tools have not been approved by HHS. This Guidance should not be treated as legal advice. Almost all states have passed laws requiring breach notification. This Guidance does not include information about state law requirements. A dental practice must be familiar with the privacy and confidentiality laws in its state whether or not the practice is a HIPAA Covered Entity. Dental practices vary widely, and each should adapt the suggestions in this Guidance to meet the circumstances it is likely to encounter. Dental practices should seek legal advice from their own attorneys on specific matters involving HIPAA, the HITECH amendments, HHS rules and regulations, and state privacy and confidentiality laws.

BREACH NOTIFICATION

Dentists have long understood the importance of safeguarding patient confidentiality. Keeping current on privacy requirements under state and federal laws can help dentists and the dental team protect their patients. Compliance can also help protect the dental practice from the legal and reputational harm that can result from an improper disclosure or use of a patient's information.

Dental practices that are HIPAA Covered Entities must implement policies and procedures to comply with the August 24, 2009 HHS Breach Notification Rule. **The Breach Notification Rule will go into effect on September 23, 2009. However, HHS has advised that it does not intend to impose sanctions for breaches that are discovered prior to February 22, 2010.** Covered Entity dental practices should implement policies and procedures to comply with the Rule by September 23, 2009.

This Guidance describes the new HHS interim final Breach Notification Rule. Under the Rule, a dental practice that is a HIPAA Covered Entity must send certain notifications in the event of a breach of a patient's unsecured PHI. Beginning on September 23, 2009, any time a dental practice that is a HIPAA Covered Entity discovers a possible breach, it must answer the following questions:

1. Is breach notification required?
2. What is the timeframe for providing notification?
3. Who should provide the notification?
4. What information should the notification contain?
5. Who should receive the notification?
6. What means should be used to provide the notification?

1. IS BREACH NOTIFICATION REQUIRED?

Breach notification is required if there has been a **breach** of **unsecured** PHI that does not fall within one of three **exceptions**.

If a HIPAA Covered Entity discovers² a possible breach, it must conduct (and **document**) a **risk analysis** to determine:

² A breach is treated as discovered as of the first day the Covered Entity **knows** of the breach, or would have known had it exercised **reasonable diligence**. A Covered Entity is not liable if it does not provide notifications of a breach that it was not aware of, unless the Covered Entity would have been aware of the breach if it had exercised reasonable diligence. A Covered Entity is deemed to have knowledge of a breach if any person (other than the person committing the breach) who is a workforce member or agent of the Covered Entity has knowledge of the breach.

- a. **Was the PHI secured or unsecured?**
- b. **Did a breach occur?**
- c. **Did it fall within an exception?**

a. **Was the PHI secured or unsecured?**

If the possible breach involved **secured PHI**, breach notification is **not** required.

If the possible breach involved **unsecured PHI**, breach notification **may be** required.

Secured PHI is PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of one or more of the methodologies specified in the Breach Notification Rule. All PHI that is **not** secured by one of these methodologies is considered **unsecured**.

Electronic PHI is considered secured if it is encrypted according to certain processes of the National Institute of Standards and Technology (NIST) and the encryption process or key has not been breached. Consult your practice management software vendor, hardware supplier, network support team, or other knowledgeable information technology professional to determine whether the necessary security methodologies are in place. Electronic PHI can also be “secured” by clearing, purging, or destroying the PHI using certain processes set by NIST.

All other PHI, including paper and film, can be secured by shredding or destroying it such that the PHI cannot be read or otherwise constructed. Any non-electronic PHI that has not been destroyed is unsecured. Oral PHI is also unsecured.

b. **Did a breach occur?**

A dentist who discovers a possible breach of **unsecured PHI** should conduct a **risk assessment** by asking the following questions. Whether or not a dentist determines that a breach has occurred, the practice should always **document** the risk assessment and include specific, fact-based reasons for the determination.

There is a **two-part test** for determining whether a breach occurred:

1) ***Did it violate the HIPAA Privacy Rule?***

If the PHI was acquired, used, or disclosed in a way that is **permitted** under the HIPAA Privacy Rule, then a breach has **not** occurred. A breach has only occurred in the event of an **impermissible** use or disclosure of PHI under the HIPAA Privacy Rule.

For example, the HIPAA Privacy Rule permits a Covered Entity to disclose the “minimum necessary” PHI to obtain payment. If a dentist discloses a patient’s PHI to his or her health plan to obtain payment, the disclosure is permitted under the HIPAA Privacy Rule and a breach has not occurred. However, if the dentist has disclosed more than the minimum necessary information to obtain payment, a breach may have occurred.

It is important for Covered Entity dental practices to implement reasonable systems for discovering breaches, because the dentist and the dental practice can be liable for failing to provide notice of a breach that an employee, independent contractor, or a Business Associate knew about (or should have known about through reasonable diligence).

2) *Is there a significant risk of harm?*

An impermissible use or disclosure that poses a **significant** risk of financial, reputational, or other harm to the individual compromises the security or privacy of the PHI and may qualify as a breach. A dentist should consider several **factors** in making this determination, including:

- **Who** impermissibly used or disclosed the information?
- **To whom** was the information impermissibly disclosed?
- Have effective steps been taken to **mitigate** the impermissible use or disclosure?

If the dentist obtains satisfactory assurance from the recipient that the PHI will not be further used or disclosed, then the impermissible use or disclosure is less likely to qualify as a breach. Such assurance may involve obtaining a confidentiality agreement from the recipient, or the recipient's assurance that the PHI will be destroyed.

- Was the PHI recovered **before** it was accessed?

For example, if a laptop containing PHI is lost or stolen and then recovered, a forensic analysis may show that the information was not opened or compromised. If there is not a significant risk of harm to the individuals whose PHI was on the laptop, the loss of the laptop would not qualify as a breach.

- What **kind** and **amount** of PHI was involved?

For example, if a Covered Entity improperly discloses the name of an individual and the fact that the individual received services, the disclosure may not pose a significant risk of harm. But if the disclosure included the type of services, or information such as an account number, social security number, or mother's maiden name, it is more likely that the disclosure could compromise the security and privacy of the information.

c. *Did it fall within an exception?*

There are three **exceptions** to the breach notification rule. If one of these exceptions applies, then a breach has not occurred and there is no need to provide notification. However, dentists should always **document** their risk assessment and include the facts show that all of the elements of an exception are satisfied.

- **Exception 1: Unintentional**

The Breach Notification Rule makes an exception for the **unintentional** acquisition, access, use, or disclosure of PHI by a workforce member or a Business Associate³ acting in **good faith** and within the **scope** of his or her authority, as long as the breach does not result in **further** impermissible use or disclosure.

³ A HIPAA "Business Associate" is an individual or entity that performs a function or activity on behalf of a Covered Entity (or performs certain services for a Covered Entity) that involves the use or disclosure of a patient's health information. Examples include claims processing or billing companies, accountants, attorneys, and administrative services firms.

For example, an individual working at a dental office mistakenly sends an e-mail containing PHI to a billing company employee. The billing company employee opens the e-mail, notices the error, and deletes the e-mail. The disclosure was unintentional, made in good faith and within the scope of the dental office worker's authority, and will not result in further impermissible use or disclosure, so a breach has not occurred.

- **Exception 2: Inadvertent**

A breach has not occurred if an individual authorized to access the PHI **inadvertently** discloses it to another person who is **authorized** to access PHI **at the same facility**, as long as the PHI is not **further** impermissibly used or disclosed. The recipient does not need to be authorized to receive the specific type of PHI that was inadvertently disclosed in order for the exception to apply. If a dental practice has several locations, the exception will apply even if the disclosure is made to an individual at another location, as long as the recipient is authorized to access PHI.

- **Exception 3: Un-retainable**

A breach has not occurred where a Covered Entity has a **good faith** belief that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to **retain** the information.

For example, a dental office sends a letter that includes PHI to the wrong individual. The letter is returned by the post office, unopened and marked as undeliverable. Under these circumstances, the PHI could not have been retained by an unauthorized recipient of the letter, so a breach has not occurred.

If a dental office assistant hands a dental chart to the wrong patient, but quickly realizes the error and retrieves the chart, a breach may not have occurred if the assistant could reasonably conclude that the patient could not have read or otherwise retained the information.

2. WHAT IS THE TIMEFRAME FOR PROVIDING NOTIFICATION?

A Covered Entity dental practice that discovers a breach of unsecured PHI must provide the required notification **without unreasonable delay** and in no case later than **60 calendar days** after the date the breach was discovered by the Covered Entity.

A dentist may take a reasonable time to **investigate** the breach and collect the necessary information before sending the notification. A dentist may also send notification in batches as information becomes available.

If a dentist compiles the information necessary to provide notification on day 10, but waits until day 60 to send the notifications, it would be an unreasonable delay (even though the notices went out within 60 days).

3. WHO SHOULD PROVIDE THE NOTIFICATION?

The Covered Entity is responsible for providing notification if a breach of its unsecured PHI is discovered, even though the breach may have been discovered or caused by an employee, independent contractor, or Business Associate.

4. WHAT INFORMATION SHOULD THE NOTIFICATION CONTAIN?

The notice must contain:

- a. A brief description of **what happened**, the date of the breach, and the date of discovery, if known
- b. A description of the **type** of unsecured PHI involved

For example, did the breach involve full names, Social Security numbers, dates of birth, home addresses, account numbers, diagnoses, disability codes, or other types of information?

The description should include only the **type** of information involved. It should be general and should describe, **but should not include**, the PHI that was breached, and should avoid using sensitive information in the notification itself.

- c. Any **steps** individuals should take to protect themselves from potential harm resulting from the breach

For example, should individuals contact their credit card companies or credit bureaus? Should they obtain credit monitoring services?

- d. A brief description of **what the Covered Entity is doing** to investigate, mitigate harm, and protect against further breaches.

For example, has the Covered Entity filed a police report (in the event of a suspected theft of unsecured PHI)? Has a workforce member involved in the breach been sanctioned?

- e. **Contact procedures** for individuals to ask questions or learn additional information.

Contact procedures must include a toll-free telephone number, e-mail address, Web site, or postal address.

The notice should be written **clearly**, at an appropriate reading level, and should not include extraneous material that may diminish the message.

Covered Entities must take reasonable steps to ensure meaningful communication to **Limited English Proficient** persons (notices may need to be translated). Effective communication with individuals who have **disabilities** may require accommodations such as providing notice in Braille, large print, or audio.

5. WHO SHOULD RECEIVE THE NOTIFICATION?

a. **The Affected Individuals**

A Covered Entity that discovers a breach of unsecured PHI must send notification to the affected individuals.

b. **The U.S. Department of Health and Human Services**

Covered Entities are also required to keep a **log of all breaches** and submit the information annually to **HHS**. If a breach involves the PHI of 500 or more individuals, the Covered Entity must notify HHS without unreasonable delay (and in no case later than 60 days from discovery of the breach). Visit

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html> for instructions.

c. Prominent Media Outlets (only if the breach involves 500 or more residents of a particular state or jurisdiction)

A breach affecting more than 500 residents of a particular state or jurisdiction must be reported to prominent media outlets serving the affected state or jurisdiction (a “jurisdiction” is a geographic area smaller than a state—for example, a county or city).

When notice to the media is required, it is **in addition to** and does not replace notice to the affected individuals.

For example, if a breach affects 200 people in Illinois, 200 people in Indiana, and 200 people in Iowa, the Covered Entity would **not** need to notify media outlets because the breach did not affect more than 500 persons in any one state. If the breach affected 600 people in Illinois and 600 people in Indiana, the Covered Entity would have to notify prominent media outlets in **both** states.

6. WHAT MEANS SHOULD BE USED TO PROVIDE THE NOTIFICATION?

• **Notice to Individuals**

A Covered Entity must provide **written notice** to the affected individuals at their last known address by **first class mail** (or by e-mail, **if** the individual has agreed to receive notice by e-mail).

In cases that the Covered Entity deems **urgent** (based on the possibility of imminent misuse of the PHI), the Covered Entity may give notice by telephone or other method. The Covered Entity that gives telephone or other notice in an urgent case must still provide written notice via mail.

If an affected individual is **deceased**, the Covered Entity should send notice to their next of kin or personal representative, if the individual gave the Covered Entity that contact information while alive.

If the affected individual is a **minor**, the Covered Entity should send notice to the minor’s parent, guardian, or legal representative.

A Covered Entity that has **insufficient or out-of-date contact information** for any of the affected individuals **may attempt to obtain** correct or updated information and send the appropriate written notice to those individuals.

Substitute notice to fewer than 10 unreachable individuals

A Covered Entity that does not have sufficient or up-to-date contact information for fewer than 10 individuals must provide substitute notice that is reasonably calculated to reach the affected individuals. The Covered Entity may provide the notice via **telephone** or **e-mail** (even if the individual has not agreed to receive notice via e-mail), or the Covered Entity may post notice in its **Web site or another location**, so long as it is reasonably calculated to reach the affected individual.

Substitute notice should be provided as soon as reasonably possible after the Covered Entity is aware that it has insufficient or out-of-date contact information for one or more individual.

Substitute notice to 10 or more individuals

A Covered Entity that has insufficient or out-of-date contact information for 10 or more individuals must post notice in one of two ways. The notice must include a **toll-free telephone number** that will remain active for 90 days for individuals to call and inquire. The two ways are:

1. Posting a conspicuous notice for a period of 90 days on the home page of its **Web** site, or
2. A conspicuous posting in a **major print or broadcast media** in geographic areas where the individuals affected by the breach likely reside.

- **Notice to HHS**

The Covered Entity must keep a log of all breaches, and report the breaches annually to HHS in the manner specified on the HHS Web site,

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.htm>

!

. The log must be maintained for a period of **six years**, and it must be available to HHS upon request. The first breach notification log must contain any breach that occurs on or after **September 23, 2009**.

If a breach affects 500 or more individuals, the Covered Entity must notify HHS without unreasonable delay (and in no event later than 60 days from the discovery of the breach). The manner of notification will be specified on the HHS Web site,

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.htm>

!

- **Notice to the Media**

HHS expects that Covered Entities will use **press releases** to report breaches affecting more than 500 residents of a particular state or jurisdiction to prominent media outlets serving the affected state or jurisdiction. The press release must be sent to a media outlet that is reasonably calculated to **reach** the affected individuals. The notice to the media must include a **toll-free number**.

How will the Breach Notification Rule affect my practice's HIPAA policies and procedures?

You will need to incorporate the requirements under the Rule into your HIPAA compliance policies and procedures. For example, you should:

- develop policies and procedures to implement the Breach Notification Rule
- train your workforce members to comply with the Rule
- have sanctions for failure to comply
- permit individuals to file complaints regarding compliance or your policies or procedures
- refrain from intimidating or retaliatory acts in connection with the Rule

Always document your compliance with the Rule. In the event of a breach, it will be your responsibility to demonstrate that all required notifications have been made. If you determine that a breach did not occur, it will be your responsibility to demonstrate how your risk assessment led to that determination.

Final Comments

The American Dental Association created this Guidance to provide dentists with tools to help their practices comply with the August 24, 2009 HHS final interim rule, *Breach Notification for Unsecured Protected Health Information*. Dental practices should keep current as further information becomes available regarding HIPAA, HITECH, and the HHS rules and regulations, as well as technical assistance and voluntary corrective action that HHS has announced it will use to work with Covered Entities to achieve compliance. HHS has not approved the Guidance and the Guidance should not be treated as legal advice. Dentists and dental practices should seek legal advice from their own attorneys on specific matters involving HIPAA, the HITECH amendments, HHS rules and regulations, and state privacy and confidentiality laws.

Reproduction and use of this material by dentists and their staff is permitted for their internal use only. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This material is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (August 31, 2009)

ADDITIONAL QUESTIONS AND ANSWERS ABOUT BREACH NOTIFICATION

What does it mean to provide “timely” notice? How much time do I have?

The Rule requires a Covered Entity to send notice “*without unreasonable delay*” but in no event later than **60 calendar days** after the date the breach was discovered. A Covered Entity should conduct a prompt investigation, taking reasonable time to investigate the circumstances of the breach in order to collect the information required to make the appropriate notification. Covered Entities may provide notice in multiple mailings (within multiple time periods) as information becomes available.

It would constitute an unreasonable delay if a Covered Entity compiles all of the necessary information on day 10, but waits until day 60 to send the notices.

If a Covered Entity conducts a prompt investigation and concludes that there was no breach, then it need not send notification, but of course it should still document its investigation and risk assessment.

What if the individual is a minor or lacks legal capacity?

If an individual affected by a breach is a minor (or otherwise lacks legal capacity due to a physical or mental condition), you should send notice to the parent or personal representative.

When can I provide notice by telephone?

In **urgent cases** involving the possibility of imminent misuse of the breached PHI you **may** give notice by telephone **in addition to** written notice.

If you have insufficient or out-of-date **contact information** for an individual, you may attempt to obtain correct or updated information by telephone, **and then send** the required written notice. In this case, though, you would not be giving notice by telephone, just asking for contact information.

If your contact information for fewer than 10 individuals is insufficient or out-of-date, you may provide **substitute notice** by telephone to each of those individuals **instead of** sending them written notification.

When using the telephone, **avoid leaving messages** with other members of the individual’s household (or on an individual’s answering machine) because doing so could be an unnecessary disclosure of PHI. If you must leave a message, limit the amount of information disclosed. For example, you could leave your name and number and indicate that you have a very important message for the individual.

Do I have to post all the information on my home page, or can I use a hyperlink that leads to the information?

You may use a hyperlink to the notice containing the required information, as long as the hyperlink is prominent—it should be noticeable given its size, color, and graphic treatment in relation to other parts of the page. The wording should convey the nature and importance of the information.

How do I decide which media outlet to notify for substitute notice?

Choose the major print or broadcast media (in the geographic area(s) where the affected individuals are likely to reside) that is most reasonably calculated to reach them. In a rural area, it may be the local newspaper. In an urban area, the newspaper serving the entire metropolitan area (or the entire state) may be more likely to reach the affected individuals. If the individuals live in different regions or state, it may be necessary to notify multiple media outlets.

The notice should be conspicuous and noticeable (similar to the home page notice discussed above) so as to be reasonably calculated to reach the affected individuals.

Is it possible that the toll-free number in my substitute notice will result in too many calls?

If you are concerned about receiving calls from unaffected individuals, include information in the notice itself to help readers determine whether their information may have been included in the breach.

I have a breach involving more than 500 individuals in a single state, and I have insufficient contact information for more than 10 of them. Do I need to provide substitute notice via print or broadcast media AND notice to the media?

A breach involving 500 or more individuals in a single state or jurisdiction requires the Covered Entity to notify prominent media outlets serving the affected state or jurisdiction. HHS expects the notification to be in the form of a press release.

If you lack sufficient or up-to-date contact information for any of the individuals, you can attempt to obtain the correct contact information for those individuals. If you succeed in obtaining the correct contact information, you may send direct written notice to those individuals.

If you still lack sufficient or up-to-date contact information for ***fewer than 10 individuals***, you can provide substitute notice to those individuals by telephone, e-mail, or by posting a notice on the home page of your Web site or in another location (as long as the notice is reasonably calculated to reach the affected individuals).

If you still lack sufficient or up-to-date contact information for ***10 or more individuals***, you are required to post substitute notice ***either*** in the form of a “conspicuous posting” in a ***major print or broadcast media*** in geographic areas where the individuals affected by the breach reside, ***or*** by posting a conspicuous notice for a period of 90 days on the ***home page of your Web site***.

The Rule appears to require that if you elect to provide the substitute notice in the media, it would be in the form of a conspicuous posting, which would be ***in addition to*** press release that you would send to the media for a breach involving more than 500 individuals.

My dental practice is in the Virgin Islands. Is that a “state or jurisdiction” for purposes of providing media notice of a breach involving more than 500 individuals?

Yes. For purposes of the Breach Notification Rule, “State” includes the 50 U.S. states, the District of Columbia, Puerto Rico, the Virgin Islands, and Guam, as well as American Samoa and the Northern Mariana Islands. A “jurisdiction” is a geographic area smaller than a state, such as a county, city, or town.

One of my Business Associates notified me of a breach involving the PHI of several different Covered Entities. Do I need to provide notice?

You need to provide written notice (or substitute notice, if contact information is insufficient or out-of-date) to any of your patients whose PHI was involved in the breach.

While the Covered Entity and not the Business Associate is ultimately responsible for assuring that appropriate notice is dispatched, in cases where the Covered Entities involved are not able to determine which entity's PHI was involved in the breach the Covered Entities may have the Business Associate provide the notification to the media on behalf of all of the Covered Entities.

How long do I have to keep documentation (such as risk assessments, copies of notices, and my breach notification log)?

Six years.

I am a Business Associate of a Covered Entity. What if I discover a breach of unsecured PHI?

In such an event you must notify the Covered Entity of the breach without unreasonable delay (and in no case more than 60 days after discovery of the breach), so that the Covered Entity can provide the appropriate notification. A Business Associate must give the Covered Entity, to the extent possible, the identity of each individual whose unsecured PHI has been breached, and any other available information that the Covered Entity is required to include in the notification. The Covered Entity may be in a better position than the Business Associate to identify the individuals affected.

A Business Associate may give the Covered Entity immediate notice of the breach and follow up with the required information as it becomes available, as long as it acts without unreasonable delay and within 60 days. If a Business Associate obtains any information after notifications have been sent (or after the 60-day period), it should still provide the information to the Covered Entity.

There was a breach at my dental practice, and a law enforcement official has instructed me to delay notification because sending notices would impede a criminal investigation. Should I comply?

Covered Entities and Business Associates must delay notification under the Breach Notification Rules if a law enforcement official determines that notification, notice, or posting would impede a criminal investigation or cause damage to national security.

If the law enforcement official provides a statement *in writing* that specifies how long a delay is required, the Covered Entity (or Business Associate) must delay notification for that period of time.

If the law enforcement official provides *oral notification*, the Covered Entity (or Business Associate) must document the statement and identity of the official and delay notification for no longer than 30 days, unless a written statement specifying the length of the delay required is received during the 30-day period.

The law of my state also provides for breach notification. Do I comply with HIPAA or state law?

A HIPAA Covered Entity must comply with HIPAA and also with any applicable state law that is *more stringent* than HIPAA. HHS advises that in most cases, Covered Entities may use a single notification to

comply with both HIPAA and any state law requirements. For example, if a state requires **additional information** to be provided in the notice, a single notice can include the information required under the Breach Notification Rule and the information required by state law.

A state law may require a different **timeframe** for notification. For example, if state law requires notice in five days, the Covered Entity can send notice in five days to comply with both the Breach Notification Rule and state law. If the Covered Entity does not have all the information required by the Breach Notification Rule, it can comply with the state law timeframe and then send the individual(s) additional notification when the additional information has been accumulated (within the timeframe provided in the Breach Notification Rule).

Is it a “breach” if a dentist has not complied with a provision of the HIPAA Security Rule?

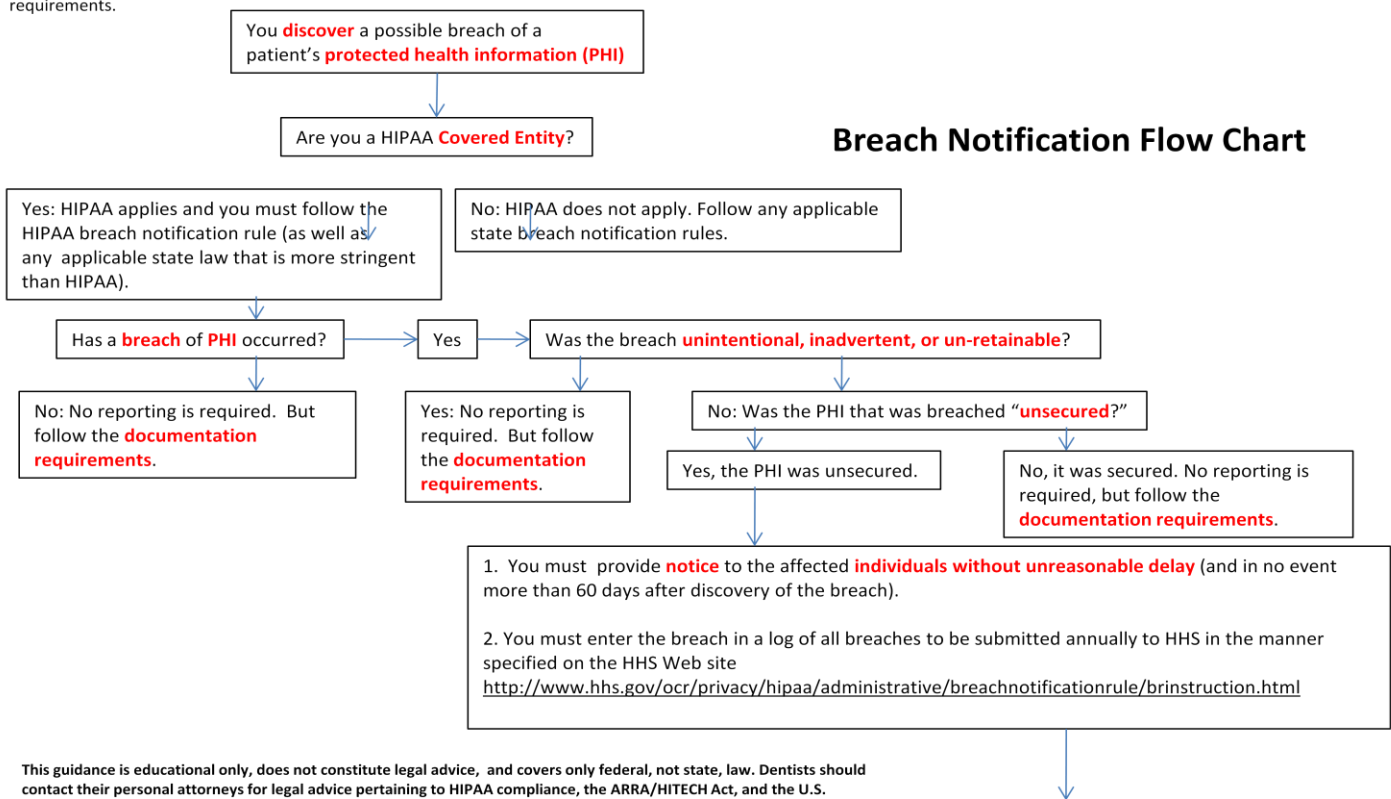
A violation of the HIPAA Security Rule **may lead to** a breach of PHI, but does not itself constitute a breach of the Breach Notification Rule. Violations of HIPAA administrative requirements (such as a lack of training) are not potential breaches, but can result in impermissible disclosures that can qualify as breaches.

Is it a “breach” if I do not secure the PHI in my practice?

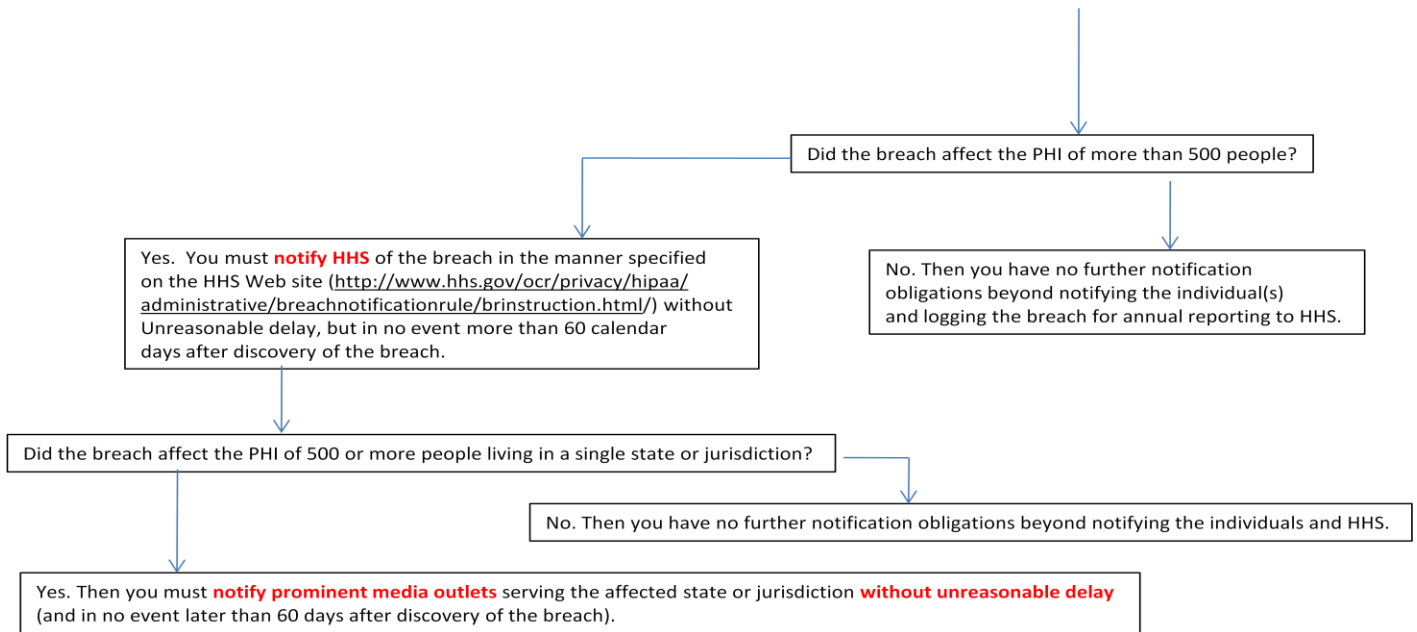
No. The Breach Notification Rule requires a Covered Entity to provide the appropriate notification in the event of a breach of unsecured PHI, but failure to secure PHI does not constitute a breach. However, securing PHI can help you avoid the possibility that you will be required to provide notification in the event of a breach.

The American Dental Association has developed the following “Breach Notification Flow Chart” to help dentists understand the new HIPAA Breach Notification Rule. On August 24, 2009, the U.S. Department of Health and Human Services (HHS) issued interim regulations entitled *Breach Notification for Unsecured Protected Health Information*. This new Rule amends the HIPAA privacy rule by requiring HIPAA Covered Entities to notify individuals, HHS, and in some cases media outlets of a breach of protected health information (PHI). **The breach notification regulations are scheduled to go into effect on September 23, 2009, although HHS has advised that it does not intend to impose sanctions for breaches that are discovered prior to February 22, 2010.** Dentists who are HIPAA Covered Entities should implement policies and procedures to comply with the Rule by September 23, 2009.

The Breach Notification Flow Chart is simplified and should only be used to gain a general understanding of the Breach Notification Rule. The “Breach Notification Glossary of Terms” defines the **Blue** highlighted terms used in the Flow Chart. The Flow Chart and Glossary of Terms should be read together in order to more fully understand the breach notification requirements.



This guidance is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (August 27, 2009)



© 2009 American Dental Association
All Rights Reserved

Reproduction and use of this material by dentists and their staff is permitted. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This guidance is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (August 27, 2009)

Breach Notification Flow Chart Glossary of Terms

*This Glossary provides information about the terms highlighted in **red** on the American Dental Association Breach Notification Flow Chart to help dentists understand the new HIPAA Breach Notification Rule. The Glossary and Flow Chart should be read together in order to more fully understand the Breach Notification Rule.*

- **Covered Entity:** A person, business, or agency that furnishes, bills or receives payment for health care in the normal course of business, and that transmits any HIPAA covered transactions electronically is a HIPAA Covered Entity. For example, a dentist who furnishes health care in the normal course of business and who submits electronic claims for payment is a HIPAA Covered Entity. A dentist is also a HIPAA Covered Entity if electronic transactions are transmitted on his or her behalf.
- **Discover:** A possible breach of protected health information (PHI) is treated as “discovered” by a Covered Entity as of the first day the breach is known (or through reasonable diligence would have been known) to the Covered Entity. If a workforce member or agent of the Covered Entity (other than the person committing the breach) knows of the breach (or would have known by exercising reasonable diligence), then the Covered Entity is deemed to have knowledge of the breach. Covered Entity dentists should implement systems for discovering breaches because they can be liable for failing to provide notice of breaches they did not know of if they would have discovered the breaches through reasonable diligence.
- **Protected Health Information (PHI):** PHI includes oral, written, and electronic information about a patient that relates to his or her health, health care, or payment for health care.
- **Unsecured PHI:** Covered Entities must provide notification when there is a breach of *unsecured PHI*. They are not required to provide notifications in the event of a breach of *secured PHI*. To be considered “secured,” PHI must be protected by the use of a methodology approved by HHS.
 - a. **Electronic PHI** is secured if it is encrypted using certain standards of the National Institute of Standards and Technology (NIST) that are approved by HHS, and the confidential encryption process or key has not been breached.
 - b. **All PHI (electronic, paper, film, etc.)** is secured if the media on which the PHI is stored or recorded have been destroyed in one of the following ways:
 - 1) Paper, film or other hard copy media have been shredded or destroyed such that PHI cannot be read or otherwise reconstructed
 - 2) Electronic media have been cleared, purged, or destroyed consisted with NIST standards approved by HHS.

Dentist should consult with their practice management software vendor, hardware supplier, network support team, or other knowledgeable information technology professionals to ascertain if an appropriate security methodology is in place for electronic PHI.

- **Breach:** There is a two-part test to determine whether a breach has occurred.
 1. Was the acquisition, access, use, or disclosure of unsecured PHI *impermissible* under the HIPAA Privacy Rule?
If a disclosure of PHI was permissible under HIPAA, then a breach has not occurred.
 2. Was there a *significant risk of financial, reputational, or other harm to the individual*?

In order to determine if an impermissible use or disclosure of PHI constitutes a breach, you will need to perform a risk assessment. You must determine if the breach poses significant risk of harm to the affected individual(s). A significant risk of financial or reputational harm to the individual is more likely if the impermissibly disclosed PHI contains information about the type of health care service the individual received (such as diagnosis, surgery, or tests) or includes information that increases the risk of identity theft. These situations create a higher likelihood that a breach has occurred.

Example 1: Your practice impermissibly discloses PHI to another Covered Entity governed by HIPAA. There may be an insignificant risk of harm to the individual, so it is less likely that a breach has occurred.

Example 2: A laptop in your office that contains PHI is stolen and then recovered. If a forensic analysis of the laptop shows that its information was not opened, altered, transferred or otherwise compromised, there may not be a significant risk of harm to the affected individuals.

- **Documentation Requirements.** Covered Entities must always document their risk assessments, even if they conclude that a breach has not occurred. The Covered Entity must be able to demonstrate that it has properly notified individuals in the event of a breach. If a Covered Entity determines that a breach did not occur, it must have a document to explain why it did not notify the individuals.
- **Unintentional, Inadvertent, or Un-retainable Disclosure:** Under the following three exceptions (or “safe harbors”), the impermissible disclosure of unsecured PHI does not constitute a breach that requires notification. A Covered Entity must always document its determination when it applies one of these exceptions.
 - **Unintentional:** If the breach was unintentional and also: (1) made by a workforce member or Business Associate, (2) acting in good faith, (3) within the scope of his or her authority, and (4) the breach does not result in further impermissible use or disclosure, then notification is not required.

A “workforce member” is defined as an employee, volunteer, trainee or other person whose conduct is under the direct control of such Covered Entity. The Covered Entity should consider whether the person was acting on its behalf at the time of the inadvertent disclosure.

A “Business Associate” is a person or entity who is not a member of a Covered Entity’s workforce and who performs, on behalf of the Covered Entity, functions or activities involving the use or disclosure of PHI. Examples of such functions are claims processing, billing, and practice management. A Covered Entity’s lawyer, accountant, and other advisors and consultants may also be Business Associates.

Example: A nurse mistakenly sends an e-mail containing PHI to a billing company employee. The billing company employee opens the e-mail, notices the error, and deletes the e-mail. The billing company employee unintentionally accessed PHI which he was not authorized to have. However, the nurse unintentionally sent the information in good faith and within the scope of her authority, and there was no further impermissible disclosure. Therefore, notification is not required.

- **Inadvertent:** Notification is not required if the breach was an inadvertent disclosure (1) by a person authorized to access PHI (2) to another person authorized to access PHI at the same facility, and (2) the PHI is not further impermissibly used or disclosed. The recipient must be authorized to access PHI, but does not need to be authorized to access the kind of PHI that was inadvertently sent.
- **Un-retainable:** Notification is not required if a Covered Entity has a good faith belief that the unauthorized person to whom the disclosure of PHI was made would not reasonably have been able to retain the information.

Example 1: A Covered Entity sends a letter that includes PHI to the wrong individual. The letter is returned by the post office, unopened and marked undeliverable. Under these circumstances, the PHI could not have been retained by an unauthorized recipient of the letter. Notification is not required.

Example 2: An office assistant hands a dental chart to the wrong patient, but quickly realizes the mistake and retrieves the chart. If the assistant could reasonably conclude that the patient could not have read or otherwise retained the information, then notification is not required.

- **Notice:** A breach of unsecured PHI requires a Covered Entity to provide notice as follows:
 - a. **Notice to Individuals:**

A covered Entity must provide written notice of a breach of unsecured PHI to the individual(s) affected at their last known address by first class mail (or by e-mail if specified by the individual).

The notice must be sent without unreasonable delay (and in no case later than 60 days after discovery of the breach).

The notice must contain:

- 1) A brief description of what happened, the date of the breach, and the date of discovery, if known,
- 2) A description of the types of unsecured PHI involved (describe, but do not include, the PHI that was breached, and avoid using sensitive information in the notification itself),
- 3) Any steps individuals should take to protect themselves from potential harm resulting from the breach,
- 4) A brief description of what the Covered Entity is doing to investigate, mitigate harm, and protect against further breaches, and
- 5) Contact procedures for individuals to ask questions or learn additional information (a toll-free telephone number, e-mail address, Web site, or postal address).

In an urgent situation, where there is the possibility of imminent misuse of unsecured PHI, the Covered Entity may notify affected individuals by telephone or other method. The Covered Entity must still provide written notice by mail.

Substitute Notice

If a Covered Entity has insufficient or out-of-date contact information for any affected individuals it may attempt to obtain correct or updated information. If it acquires the contact information, it can send written notice.

If a Covered Entity still lacks contact information for fewer than 10 individuals, it must provide substitute notice that is reasonable calculated to reach the affected individuals via e-mail or telephone, or by posting a notice on its Web site or another location.

If a Covered Entity lacks contact information for 10 or more individuals, it is required to post a notice that includes a toll-free telephone number (active for 90 days) that individuals can call to inquire. The notice can be posted by either:

- a) posting a conspicuous notice for a period of 90 days on the homepage of the Covered Entity's Web site, or
- b) a conspicuous posting in a major print or broadcast media in geographic areas where the individuals affected by the breach reside.

b. Notice to HHS:

- Every Covered Entity must keep a log of all breaches and report the breaches annually to HHS in the manner specified on the HHS Web site, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/binstruction.html>.
- For any breach affecting 500 or more individuals, the Covered Entity must notify the Secretary of the U.S. Department of Health and Human Services (HHS) without unreasonable delay, but in no case later than 60 days after discovery of the breach, in the manner specified on the HHS Web site <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/binstruction.html>.

c. Notice to Media:

If a breach affects more than 500 residents of a particular state or jurisdiction, the Covered Entity must notify *prominent media outlets* serving the affected state or jurisdiction. The notification must be given without unreasonable delay, and in no case later than 60 days after discovery of the breach. When notification to media outlets is required, it is in addition to, and does not replace, notice to the affected individual(s).

Example 1: If a breach affects 200 people in Illinois, 200 people in Indiana and 200 people in Iowa, the Covered Entity would *not* need to notify prominent media outlets because the breach did not affect more than 500 persons in any one state (but the Covered Entity would still need to provide notice to those individuals).

Example 2: If a breach affected 600 people in Illinois and 600 people in Indiana, you would have to notify prominent media outlets in both states in addition to providing notice to the affected individuals.

- **Without Unreasonable Delay:** HHS expects Covered Entities to make individual notifications as soon as reasonably possible. A Covered Entity may take *reasonable* time to investigate the circumstances surrounding the breach. However, the time period for breach notification begins when the incident is discovered, not when the investigation of the incident is complete. A Covered Entity must send the required notification in no case later than 60 days after the date it discovered the breach.

Example: You learn of a possible unauthorized use or disclosure of PHI and on day 10 your investigation reveals that a breach has occurred. It would constitute an unreasonable delay if you waited until day 60 to notify the individuals.

© 2009 American Dental Association

All Rights Reserved

Reproduction and use of this material by dentists and their staff is permitted for their internal use only. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This material is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (August 31, 2009)

SAMPLE DENTAL PRACTICE BREACH NOTIFICATION ACTION LIST

IMPORTANT NOTE: While this sample action list attempts to provide dentists with certain tools needed to comply with the Breach Notification Rule, it has not been approved by the U.S. Department of Health and Human Services (HHS). It should not be treated or considered as legal advice or as applicable to any dental practice. Rather, each practice should adapt this model Action List in light of its own experience and the advice that it receives from counsel.

Anytown Dental Center

Breach Notification Compliance Action List

1. Confirm that our practice is a HIPAA Covered Entity
2. Become familiar with the Breach Notification Rule and any applicable state law requirements
3. Develop a breach log for annual reporting to HHS (any breach discovered on or after September 23, 2009 must be logged for annual submission to HHS; breaches involving 500 or more individuals must be reported without unreasonable delay, and in no case later than 60 days after discovery).
4. Develop Breach Notification policies and procedures
 - a. Review all PHI in our practice (electronic, paper, oral, or in any other form)
 - b. Determine how we store PHI and whether it is "secured" under the Breach Notification Rule
 - c. Develop procedures for reasonable diligence to discover breaches
 - d. Assign responsibility for responding to discovery of a breach
 - e. Develop procedures to respond to discovery of a breach:
 - 1) Develop risk assessment and documentation procedures
 - 2) Develop forms to use for notification:
 - a) written notice forms for affected individuals
 - b) substitute notice forms to use when contact information is insufficient or not up-to-date
 - c) model press release for breaches involving more than 500 individuals
 - 3) Institute sanctions for workforce members who violate the Rule and our dental practice's breach notification policies and procedures
 - f. Train workforce to comply with the Breach Notification Rule and our new policies and procedures
 - g. Review Business Associate Agreements that are already in place (and the standard form our practice uses with Business Associates) to make sure these documents comply with the Rule and protect our practice in the event the Business Associate discovers a breach. For example, the Business Associate Agreement can provide:
 - 1) Timeframe requirements for a Business Associate to notify our practice of a breach
 - 2) Specific obligations for each party
 - 3) Provisions to avoid confusing duplicate notices to individuals
 - 4) Requirements for securing PHI
 - 5) Indemnification provisions in the event the Business Associate causes a breach or violates the Breach Notification Rule or the Business Association Agreement
 - h. Review how our practice collects and maintains patient contact information
 - 1) Do we ask patients to update their contact information regularly?
 - 2) Do we asking patients whether notices may be sent via e-mail in the event of a breach

- 3) Does our practice have up-to-date contact information for parents, guardians, or other legal representatives?
 - i. Consult with our practice management software vendor, hardware supplier, network support team, or other knowledgeable information technology professional to ascertain whether an acceptable security methodology is in place
 - j. Determine how our practice Web Site could be used to post substitute notice in the event of a breach affecting individuals for whom we lack contact information.
 5. Schedule an appointment with the attorney for our practice to review our compliance policy and procedure, and to discuss any questions that arise concerning HIPAA, HITECH, the HHS rules and regulations, and any applicable state privacy and confidentiality laws.

© 2009 American Dental Association

All Rights Reserved

Reproduction and use of this material by dentists and their staff is permitted for their internal use only. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This material is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (August 31, 2009)

Sample Breach Notification Policy and Procedures

IMPORTANT NOTE: The following sample policy and procedures demonstrates how a practice might comply with the Breach Notification Rule. While this sample attempts to provide dentists with certain tools needed to comply with the Breach Notification Rule, it has not been approved by the U.S. Department of Health and Human Services (HHS). It should not be treated or considered as legal advice or as applicable to any dental practice. Rather, each practice should adapt policies and procedures in light of its own experience and the advice that it receives from counsel.

Anytown Dental Center

Breach Notification Policy and Procedures

Anytown Dental Center has adopted a Breach Notification Policy and Procedures Program (“Program”) pursuant to HITECH Act of the American Recovery and Reinvestment Act of 2009 and the rules and regulations issued by the U.S. Department of Health and Human Services (“HHS”). The purpose of the Program is to detect possible breaches of PHI, conduct a risk assessment to determine whether a breach of unsecured PHI has occurred, and provide any required notification. This Program must be observed by all employees, agents, and independent contractors of this practice, including the professional, administrative, and clerical staff (the “Workforce”).

I. **Discovering Possible Breaches**

The Workforce will exercise reasonable diligence to discover any possible breach of PHI. When a member of the Workforce has knowledge of a possible breach, he or she will **immediately** notify the Office Manager of the possible breach and the date it was discovered. Sanctions, up to and including possible termination, will apply to a Workforce member who has knowledge of a possible breach and fails to notify the Office Manager.

II. **Risk Assessment**

Upon discovering a possible breach, or receiving notice of a possible breach, the Office Manager will investigate and conduct a risk assessment to determine whether a breach of unsecured PHI has occurred. The Office manager will **document** the risk assessment **whether or not** the risk assessment reveals that a breach has occurred.

III. **Mitigation**

If the Office Manager determines that a breach of unsecured PHI has occurred, the practice will take steps to mitigate the breach and any harm that is likely to result from the breach. The practice will take steps to prevent breaches from occurring in the future.

IV. **Breach Log**

The Office Manager will keep a log of all breaches and report annually to HHS in the manner specified on the HHS Web site, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.

V. **Notification**

- A. Names and Information.** If a breach of unsecured PHI has occurred, the Office Manager will collect the names and contact information for individuals affected by the breach and the information required for the notification.
- B. Urgent Situation.** In an urgent situation involving the possibility of imminent misuse of unsecured PHI, the Office Manager may notify affected individuals by telephone in addition to providing written notice.
- C. Timing of Notice.** The notice will be sent without unreasonable delay, and in no case later than 60 days after the discovery of the breach.
- D. Contents of Notice.** The notice will include a brief description of what happened, including the date of the breach and the date of discovery, if known, a general description of the types of unsecured PHI was involved, any steps individuals should take to protect themselves from potential harm resulting from the breach, a brief description of what the practice is doing to investigate, mitigate harm, and protect against future breaches, and contact procedures for individuals to ask questions or learn additional information (including telephone number, e-mail address, Web site, postal address, or toll-free telephone number, as appropriate).

IMPORTANT: The notification must not include any PHI or any other sensitive information.

- E. Means of Sending Notice.** The Office Manager will provide written notice to each affected individual. Notices will be sent by e-mail to all individuals who have so specified. All other individuals will be notified by first-class mail to their last known address.
- F. Unreachable Individuals.** If the practice lacks contact information for any affected individual, the Office Manager will attempt to obtain current contact information so that appropriate notices may be sent.

If the practice is unable to obtain current contact information for fewer than 10 individuals, the Office Manager may provide substitute notice that is reasonably calculated to reach them via telephone, e-mail, or by posting a notice on the practice Web site or in another location.

If the practice is unable to obtain current contact information for 10 or more individuals, the Practice Manager will post a conspicuous notice for 90 days on the home page of the practice Web site that includes a toll-free telephone number for individuals to call to inquire. The toll-free number will remain active for 90 days.

- G. More than 500 Individuals.** If the unsecured PHI of more than 500 individuals is breached, the Office Manager will notify HHS without unreasonable delay (and in no case later than 60 days after discovery of the breach) in the manner specified on the HHS Web site <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.
- H. More than 500 Individuals in a state or jurisdiction.** If a breach of unsecured PHI affects more than 500 individuals in a single state or jurisdiction, the Office Manager will send a press release to prominent media outlets serving the affected state or jurisdiction, in addition to providing notification to the affected individuals and HHS. The press release will be sent without unreasonable delay and in no case later than 60 days after discovery of the breach, and will contain a toll-free number for individuals to call and inquire.

VI. Plan Administration and Updates

All members of the Workforce of this practice will receive a copy of this Policy and will be instructed as to its procedures. The Practice will ask each employee to sign an acknowledgement of receipt and

understanding. We will evaluate our Program annually and update it in light of experience. Any questions about this Policy should be addressed to the Office Manager.

ACKNOWLEDGEMENT
(to be completed by all members of the Workforce)

I, _____, have read the practice's Breach Notification Policy and Procedures and understand the contents. I have been instructed regarding situations that may suggest a possible breach of PHI as described in the Breach Notification Policy and Procedures. If I discover a possible breach of PHI, I will immediately bring the matter to the attention of the Office Manager.

By: _____

Print name

Date: _____

Approved by: _____

Name: _____

Title: _____

Effective date: _____

Review Date: _____

© 2009 American Dental Association

All Rights Reserved

Reproduction and use of this material by dentists and their staff is permitted for their internal use only. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This material is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (September 2, 2009)

SAMPLE BREACH NOTIFICATION RISK ASSESSMENT WORKSHEET

IMPORTANT NOTE: The following sample worksheet demonstrates how a practice might document its risk assessment as required by the Breach Notification Rule. While this sample worksheet attempts to provide dentists with certain tools needed to comply with the Breach Notification Rule, it has not been approved by the U.S. Department of Health and Human Services (HHS). It should not be treated or considered as legal advice or as applicable to any dental practice. Rather, each practice should adapt this sample worksheet in light of its own experience and the advice that it receives from counsel.

Background: When Dr. Smith, owner of the Dental Center of Anytown, arrived at work on the morning of September 23, 2009, she discovered that a burglar had broken into the dental office. Dr. Smith immediately called the police. An investigation revealed that the burglar had apparently attempted to obtain prescription pads, narcotics, and cash. These items were securely locked and an inventory revealed that nothing was missing. However, documents with the names and credit card numbers of three patients had been left on a desk in the business office, which the burglar had entered by breaking a door lock.

*Dr. Smith conducted a risk assessment using the following **Risk Assessment Worksheet** and determined that a breach had occurred. She determined that this was an urgent case (based on the imminent misuse of unsecured PHI) because credit card numbers were involved, so she chose to provide prompt notice by telephone, which is in addition to the required written notice.*

*Dr. Smith logged the incident and sent written notice to each of the three patients pursuant to the Breach Notification Rule (see the following **Sample Breach Notification Notice to Individual**). The notice is required to contain (1) a brief description of what happened, including the date of the breach and the date of discovery if known, (2) a description of the type of unsecured PHI involved, (3) any steps affected individuals should take to protect themselves from potential harm resulting from the breach, (4) a description of what the Covered Entity is doing to investigate, mitigate harm, and protect against future breaches, and (5) contact procedures for individuals to ask questions or learn additional information.*

ANYTOWN DENTAL CENTER

BREACH NOTIFICATION RISK ASSESSMENT WORKSHEET

This worksheet must be completed for each possible breach of PHI of a patient of our dental practice.

1. What happened? What type of PHI was involved?

On the morning of September 23, 2009, we arrived at the Dental Center and discovered that it had been burglarized. The door had been forced in, the door lock to the business office was broken. The names and credit card numbers of three patients were

on a document on a desk in the business office, and the burglar may have had a chance to copy them.

2. Was the PHI secured?

No, it was a paper document.

3. Was there a breach? Answer questions a, b, and c, then conclude if there was a breach.

a. Was it permissible under HIPAA? Yes No

If it was permissible under HIPAA, explain:

b. Is there a significant risk of harm? Yes No

Consider:

- Who made the breach? To whom?
- Have effective steps been taken to mitigate?
- Was the PHI recovered before it was accessed?
- What kind and amount of PHI was involved

Explain:

It involved credit cards numbers.

c. Did it fall within an exception?

- ✓ Was it unintentional, by a workforce member or a Business Associate acting in good faith and within the scope of his or her authority, and will not result in further impermissible use or disclosure?

Yes No

If yes, explain:

- ✓ Was it inadvertent, by a person authorized to access the PHI to another person who is authorized to access PHI our facility, and the PHI is not further impermissibly used or disclosed?

Yes No

If yes, explain:

- ✓ Do we believe in good faith that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to **retain** the information.

Yes No

If yes, explain:

CONCLUSION: Was there a breach? Yes No

4. What is our dental practice doing to investigate, mitigate harm, and protect against future breaches?

- ✓ Notified the police
- ✓ Urgent, so called affected patients on the phone (in addition to written notice)
- ✓ Looking into prevention measures, including alarm system.

5. Were 500 or more individuals involved? Were 500 or more in one state or jurisdiction?

Yes No

Explain:

3 people were involved

© 2009 American Dental Association

All Rights Reserved

Reproduction and use of this material by dentists and their staff is permitted for their internal use only. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This material is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (September 2, 2009)

Sample Breach Notification Notice to Individual

Dr. Smith
Dental Center of Anytown
123 Any Road
Anytown, U.S.A.

Mrs. Jane Doe
123 Doe Street
Anytown, U.S.A.

September 24, 2009

Dear Mrs. Doe:

As we discussed in our telephone conversation yesterday, on the morning of September 23, 2009 our practice discovered that a burglar had entered our dental office during the previous night. The burglar may have had access to the names and credit card numbers of three of our patients, including yours.

You should take the following steps to protect yourself from harm that could result from this breach of your information:

- Immediately notify your credit card company that your credit card number may have been copied.
- Follow your credit card company's instructions.

When we discovered that our dental office had been burglarized we immediately contacted the police. We are notifying the three individuals who may have been affected by this incident, and we are developing new office procedures to prevent such events in the future, including the installation of an alarm system.

If you have any questions or require additional information about this matter, please do not hesitate to contact me by telephone at XXX-XXX-XXXX, by email at xxx@xxxxx, or by post at the above address.

Very truly yours,

Dr. Smith

© 2009 American Dental Association

All Rights Reserved

Reproduction and use of this material by dentists and their staff is permitted for their internal use only. Any other use, duplication or distribution of this material by any other party requires the prior written approval of the American Dental Association.

This material is educational only, does not constitute legal advice, and covers only federal, not state, law. Dentists should contact their personal attorneys for legal advice pertaining to HIPAA compliance, the ARRA/HITECH Act, and the U.S. Department of Health and Human Services Regulations. (September 2, 2009)