

## NEW HIPAA REQUIREMENTS: BREACH NOTIFICATION

Under new federal rules, employer-sponsored group health plans must provide notification to affected individuals, the government and, in some cases, the media if a breach occurs with respect to certain protected health information. That may sound simple enough, but the notification process is complex and it can be a public relations nightmare. No one likes to hear that their personal information may have been compromised.

With some advance planning, employers can minimize the chances of a breach that would require notification under the new rules. Crucial facets of that advance planning are highlighted below.

The new rules, issued by the U.S. Department of Health and Human Services, apply to entities covered by the privacy and security requirements of the Health Information Portability and Accountability Act (HIPAA). The breach notification requirements build on existing privacy and security requirements, using several definitions and concepts that will likely be familiar to health plan sponsors.

The new rules do not require plans to implement new security measures or prohibit previously permissible uses and disclosures of health information. The notification requirements do, however, create strong incentives for plans to secure protected health information (PHI) and to carefully monitor any uses and disclosures of health information that are not explicitly permitted.

### EFFECTIVE DATE: SEPTEMBER 23, 2009

The breach notification requirements were enacted earlier this year as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which specified that they would become effective 30 days after HHS issued implementing regulations. That happened on August 24, 2009, making the rules effective with respect to breaches occurring on or after September 23, 2009.

### PENALTY DATE: FEBRUARY 22, 2010

According to HHS, "it will take...time to implement the processes and procedures necessary to comply" with the new rules. Therefore, HHS promises in the preamble to the new regulations that it will not impose sanctions for noncompliance with respect to breaches discovered before February 22, 2010. HHS cautions, however, that this is not an extension of the effective date, and compliance is expected with respect to any breach occurring on or after September 23, 2009.

Before February 22, 2010, employers may wish to review plan operations from September 23, 2009 forward to determine if any events have occurred that might be construed as breaches (defined below). Notification requirements apply to breaches occurring on or after September 23, 2009, but no penalties will be applied to notification failures with respect to breaches discovered before February 22, 2010. A plan will lessen its exposure by documenting its discovery before February 22, 2010 of any occurrences since September 23, 2009 that might be breaches. In addition to reviewing their own health plan operations, employers may want to require TPAs and other third-party service providers to conduct a similar review and report any occurrences to the plan's privacy and security official(s).

## WHAT IS REQUIRED?

The basic requirement is to provide prompt notification to affected individuals and HHS if a breach occurs in the course of a plan's operations with respect to unsecured protected health information. (In some cases, media notification also is required.) The rules also require plans to implement several administrative measures to make sure the plan detects breaches and provides required notification.

### CHECKLIST:

The steps required to bring an employer's health plans into compliance with the breach notification rules' administrative requirements include:

- Identify all plans providing health benefits; determine whether any plans are exempt or can qualify as "shortcut" plans, and document those determinations
- For non-shortcut plans:
  - Determine the extent to which insurers providing plan benefits will be responsible for providing notification and the extent to which the plan prefers to assign breach notification to third-party service providers
  - Determine the plan's policy on encrypting and destroying PHI according to HHS standards
  - Define the occurrences that the plan's workforce members and business associates are responsible for reporting, as well as timing and means of reporting
  - Identify the individual(s) who will decide whether a particular occurrence is a breach and whether notification is required
  - Identify each plan's workforce and provide training as appropriate to each workforce member regarding the impact that breach notification compliance measures will have on his or her duties
  - Determine whether revisions to business associate contracts are needed, and, if so, negotiate revisions to:
    - ◆ Require plan service providers to report occurrences when the plan determines they should be reported and in the manner the plan determines reporting should occur
    - ◆ Require encryption or destruction of PHI that the business associate handles according to the plan's preferences
    - ◆ Provide for performance of any breach notification functions that the plan elects to delegate to a service provider
  - Create and implement written policies and procedures covering (or revise existing privacy and security policies to include):
    - ◆ Encryption and destruction of health information so that it is deemed secure
    - ◆ Detection, reporting and evaluation of events that might be breaches
    - ◆ Provision of any required breach notification
    - ◆ Training workforce members on new/revised policies and procedures
    - ◆ Provisions to be included in business associate agreements
    - ◆ Receipt and documentation of complaints in connection with breach notification
    - ◆ Sanctions for violations of the plan's policies and procedures
    - ◆ Prohibition of intimidation, retaliation and requirements to waive breach notification rights as a condition of enrollment or receiving benefits
    - ◆ Creation and retention of documentation sufficient to demonstrate compliance
  - Determine whether any changes to the plan's practices necessitate changes to its notice of privacy practices and, if so, revise and reissue the notice
  - Create and maintain documentation of compliance

## CALLING ALL GROUP HEALTH PLANS

Any employer-sponsored plan that is subject to the HIPAA privacy and security rules is also subject to the breach notification rules. In this case, “plan” refers to an ERISA plan (or an equivalent governmental or church plan), so a single plan may encompass several different health and non-health benefits programs. (For an extensive discussion of which plans are subject to the HIPAA privacy rules, see Chapter 10 of Willis’ online compliance manual.)

HIPAA veterans will recall that virtually all employer plans that provide any health benefits are subject to the privacy and security requirements, including:

- Governmental and church plans
- Small plans of small employers
- Health flexible spending accounts under cafeteria plans
- Dental and vision plans

In fact, the only health plans that are completely exempt are plans with fewer than 50 participants that have no outside administrator (i.e., the employer processes and pays all claims in-house without any outside assistance).

Employers should review their existing HIPAA privacy and security documentation to ensure that all health benefits offered to employees (and all group health plans) have been identified and any applicable exemptions have been documented.

## SHORTCUT PLANS GET A BREAK

Under HIPAA, shortcut plans get a break on complying with the breach notification rules. The shortcut applies to a plan under which:

- All health benefits are fully insured (i.e., the plan provides no self-insured health benefits)
- The sponsoring employer generally does not create or receive any health information in connection with the plan (subject to narrow exceptions for certain types of information, including enrollment information and information provided under an authorization)

Just as with privacy compliance, the insurers providing coverage under shortcut plans are responsible for complying with the breach notification requirements in connection with their own operations. Meanwhile, the employer-operated parts of shortcut plans do not receive any information that could result in a breach. In effect, the employer can rely on the insurer for breach notification compliance and does not need to provide breach notification, adopt related policies and procedures, enter into business associate agreements, or complete any of the other administrative requirements of the breach notification rules.

Caution: Shortcut plans that avoid obligations under the terms of HHS’ regulations may still have breach notification obligations assigned to them under insurance policies. In other compliance contexts, insurers have included policy provisions assigning compliance with notification requirements to the employer. This type of delegation may also occur in connection with the breach notification rules. (For an extensive discussion of shortcut plans, see Chapter 10 of Willis’ online compliance manual.)

Employers are not entirely free of breach notification requirements with respect to shortcut plans, however. They must ensure that individuals exercising their HIPAA rights are not subject to intimidation or retaliation, and that plan enrollment and benefits are not conditioned on waiver of breach notification rights.

Employers should review their existing HIPAA privacy documentation to ensure that it reflects current insurance and plan arrangements and that any shortcut plans previously identified continue to meet the requirements.

## WHEN BREACH NOTIFICATION IS REQUIRED

Breach notification generally is required when a group health plan discovers that a breach has occurred with respect to unsecured protected health information. A breach that would require notification can occur in connection with the employer's operations under the plan, but can also occur in the course of a service provider's activities. Under the breach notification rules, a service provider that is a business associate must notify the plan of any breach occurring in its operations. The plan, in turn, is required to provide any required notification regarding that breach to affected individuals, HHS, and, if applicable, media outlets.

Since group health plans must provide notification regarding breaches that occur in the business associates' operations, identifying business associates is an important compliance step. The service providers that are business associates for purposes of HIPAA privacy and security are also business associates for purposes of breach notification. (For an extensive discussion of which service providers are business associates, see Chapter 10 of Willis' online compliance manual.)

When considering an employer's obligations with respect to business associates' operations, keep in mind that an insurer providing health insurance coverage under an employer-sponsored plan is not a business associate for that plan, so the plan and the employer sponsoring it generally have no responsibility to provide notification regarding breaches occurring in the insurer's operations (unless the employer or plan agrees to do so). However, an insurer providing administrative services under an employer-sponsored plan (e.g., claim processing) usually is a business associate and the normal business associate rules apply.

Employers should review their existing HIPAA privacy and security documentation to ensure that all service providers have been identified and business associate contracts executed as required. It may be unnecessary to amend business associate contracts to reflect the breach notification rules. Business associate contracts already in place under the privacy and security rules must require the business associate to report security incidents as well as uses and disclosures that are not permitted under the terms of the business associate contract. As explained below, however, revisions to existing business associate contracts may be desirable.

## WHAT IS A BREACH?

An occurrence qualifies as a breach under the new HHS rules only if the answer to all five of these questions is "yes."

1. Is protected health information (PHI) involved?
2. Was there a use or disclosure of PHI?
3. Was there a violation of the privacy rules?
4. Was the security or privacy of the PHI compromised?
5. Are all three exceptions inapplicable?

Prompt and careful review of a possible breach event against this definition will be needed to decide whether notification is required. (Taking too much time to analyze whether an event is a breach may make the notification late, so any review must occur swiftly after a possible breach event is discovered.)

**1. Is Protected Health Information Involved?** Unless an event involves PHI, it cannot be a breach. Employers will recall that HIPAA defines PHI very broadly and that PHI generally includes almost all individually identifiable health information that is created or received by a group health plan or by an employer or service provider in connection with a group health plan. One important exception to this rule relates to an employer's handling of enrollment information. Employers can generally create, use, and, within limits, disclose enrollment information without treating it as PHI.

**2. Was There a Use or Disclosure?** The terms “use” and “disclosure” have the same meaning for purposes of defining the term breach as they do for purposes of HIPAA privacy and security. They encompass several activities.

- **Disclosure.** PHI is disclosed upon the release, transfer, provision of access to or divulging in any other manner of the PHI.
- **Use.** PHI is used if it is shared, employed, applied, utilized, examined or analyzed.

In other words, someone must at least gain access to the PHI for the notification requirements to apply. Simply having inadequate security measures or faulty privacy policies and procedures will not trigger notification, so long as no one uses or discloses PHI. Keep in mind that the person using or disclosing the information need not be associated with the health plan (e.g., a thief who has stolen a laptop may use PHI by examining unencrypted files that contain claim payment information).

**3. Was There a Violation of the Privacy Rules?** No breach occurs unless a use or disclosure of PHI violates the privacy rules. Mere failure to comply with administrative requirements of the privacy rules (e.g., lack of written policies and procedures or failure to train workforce members) will not by itself trigger breach notification requirements. A use or disclosure of PHI must constitute a violation of the privacy rules for notification to be required.

As described above, no violation of the privacy rules occurs (so no notification requirement can be triggered) when an employer uses or discloses enrollment information. Likewise, use or disclosure of information that has been de-identified according to HIPAA standards cannot violate the privacy rules because it is not PHI. Two additional types of information are always insulated from full compliance with the privacy rules: summary health information (which is very similar to de-identified information) when used for limited purposes and information used or disclosed in accordance with a HIPAA-compliant authorization. An employer can use or disclose these four types of information (subject to the restrictions noted) without violating the privacy rules.

**4. Was the Security or Privacy of the PHI Compromised?** This element of the breach definition means that a use or disclosure of PHI that violates the privacy rules will not trigger breach notification requirements unless it also “poses a significant risk of financial, reputational, or other harm to the individual.” To determine the risk, a plan would perform a risk assessment that takes into account such factors as:

- What type or amount of PHI was impermissibly used or disclosed (e.g., information that a payment was made for an individual’s hospital stay compared to an itemized bill for the hospital stay)
- Who impermissibly used the PHI (e.g., a member of the employer’s HR department who has agreed not to disclose it compared to an individual’s direct supervisor)
- To whom was the PHI impermissibly disclosed (e.g., another health plan which is subject to HIPAA privacy requirements compared to a life insurance company which is not)
- What steps have been taken to mitigate any harm that might be caused by the impermissible use or disclosure (e.g., all possible recipients have agreed to destroy the PHI received and refrain from further disclosure)

**5. Are All Three Exceptions Inapplicable?** The new rules identify three narrow exceptions to the definition of breach.

- **Unintentional Use.** No breach occurs if a workforce member or a business associate’s employee, acting in good faith and in the course of job duties, impermissibly accesses or uses information, provided the event does not result in further use or disclosure of the information in violation of the privacy rule. HHS gives the example of a misdirected e-mail. The recipient, an employee of the same company as the sender, reads the e-mail, realizes the misdirection, alerts the sender, deletes the e-mail, and does not use or disclose the protected health information in the misdirected e-mail.

- **Disclosure to Authorized Recipient.** No breach occurs if someone who is authorized to access PHI held by a plan impermissibly discloses PHI to someone else who is also authorized, provided the recipient does not further use or disclose the PHI in violation of the privacy rules. An example might be an e-mail regarding a disputed claim that includes the claimant's name and several details of the medical services received. A workforce member sends the e-mail to an employee at the TPA. The recipient realizes that the individual's name and details of the services are not needed to analyze the issue presented. Before responding, the recipient deletes all identifying information and unnecessary health information from the e-mail (including previous e-mails forwarded with the response).
- **Disclosure Not Retained.** No breach occurs if the plan has a good faith belief that the unauthorized recipient of a disclosure would not reasonably have been able to retain the information disclosed. HHS gives the example of a misdirected EOB that is returned to the plan unopened.

Employers implementing the breach notification requirements for their health plans will want to make sure that these five questions are asked regarding any incident that is a potential breach, so that notification is provided only when required. Plans' policies and procedures should call for this analysis. The analysis of each incident should be documented, especially if the plan concludes that the incident was not a breach.

When implementing the breach notification requirements, an employer might assign this analysis to individual workforce members and business associates so that they report to the plan's privacy and security official(s) only those incidents that they conclude are, or appear very likely to be, breaches. Employer-sponsored plans may be best served, however, by requiring workforce members and business associates to report all uses and disclosures that are not clearly permissible to the plan's privacy and security official(s). Those individuals would perform and document the breach analysis for all reported events.

This approach is suggested because the rules put the burden on health plans to prove that all required breach notifications have been provided. Overly inclusive reporting of incidents, with a few individuals making and documenting all determinations about whether a breach has occurred, will facilitate gathering that proof and applying the criteria consistently. Regardless of the approach, a plan's policies and procedures and business associate agreements should be amended as needed to incorporate the desired detection, evaluation, and reporting.

## NOT ALL BREACHES REQUIRE NOTIFICATION

If PHI has been secured according to HHS guidance, then no breach notification requirements apply to any use or disclosure of that PHI, even if the use or disclosure would otherwise qualify as a breach. Despite the term, "securing" PHI in this context does not refer to complying with the HIPAA security rules. It refers to using specific measures to make the PHI unusable, unreadable or indecipherable in the event of impermissible use or disclosure. For example, theft of a laptop would not require breach notification if all PHI on the laptop were encrypted according to HHS criteria. HHS guidance specifies that encryption and destruction are the only means of securing PHI.

- **Electronic PHI.** HHS guidance specifies that for data to be secured, encryption must meet NIST (National Institute of Standards and Technology) standards, and the decryption key must be stored separate from the encrypted information. Similarly, destruction of electronic information requires that it be "cleared, purged, or destroyed" consistent with NIST standards.
- **Other PHI.** Information on paper or other hard copy is not secured unless it has been shredded or otherwise destroyed so that it cannot be read or reconstructed. HHS does not provide any means of securing conversations or other non-written PHI.

A health plan's PHI cannot be secured at all times, so it is not possible to adopt security measures that will preclude breach notifications. Securing PHI to the extent feasible, however, will minimize the chances that breach notification will be required.

Employers should consult with their information technology professionals to determine whether encryption according to the NIST standards is feasible for the electronic PHI that the employer maintains. In addition, employers should implement PHI destruction procedures that render discarded PHI secure. Business associate agreements – particularly those with claim administrators – should require encryption according to the HHS standards for all electronic PHI and compliance with the HHS standards for destruction when disposing of PHI.

## DISCOVERY TRIGGERS NOTIFICATION

The time for providing notification begins running when a breach is discovered. Under the new rules, “discovery” may occur much sooner than might be expected, meaning that very little time to gather information and provide notification may remain when the privacy or security official learns of a breach.

- Discovery of a breach occurs when the plan discovers the event that may constitute a breach, not when the plan determines that the event constitutes a breach that requires notification. For example, discovery occurs on the day that the plan learns that a laptop is missing, not on the date three days later when it is determined that the laptop contains unencrypted PHI.
- A health plan discovers a breach on the date that it is known, or by exercising reasonable diligence, would have been known. If a health plan does not have a system for detecting and reporting impermissible uses or disclosures of PHI, for example, it might be deemed to have discovered a breach much earlier than the privacy or security official actually learned of it.
- The plan is deemed to know everything that its workforce members and other agents (except the workforce member or agent committing the breach) know or, with the exercise of reasonable diligence, would know.
  - **Workforce Members.** Health plans other than shortcut plans are required by the privacy rules to identify in their plan documents (by title or name) the “designated employees” within the sponsoring employer’s workforce. These designated employees are the plan’s workforce members. The plan is treated as discovering a breach at the moment that any of these employees (other than one committing the breach) knows – or, with the exercise of reasonable diligence, would know – of an event that may constitute a breach and the time to provide notification begins running.
  - **Agents.** The regulations refer to “federal common law” for the definition of an agent, meaning that the term is not clearly defined but has something to do with having a third party act on behalf of and at the direction of the plan. HHS has noted that, in some cases, a business associate (e.g., a TPA) may be an agent of the health plan. If a TPA were a health plan’s agent, the plan would be deemed to know whatever the TPA knows about a breach, even before the TPA reports the information to the plan.

## TIMING

Notification is required without unreasonable delay (and in no event later than 60 days) after a health plan discovers that a breach has occurred. The primary requirement is to provide notice without unreasonable delay, taking into consideration a prompt investigation of an incident and collection of the information needed for any required notification. The 60-day period is an outside limit, and HHS notes that taking the full 60 days to provide notification may constitute unreasonable delay. The regulations provide for notification to be delayed at the request of law enforcement officials in some cases.

The rules put the burden on the plan to prove (presumably by documentation prepared when an event was discovered and as it was investigated) that notification was made by the time required. Because the time begins running when an event would have been known to a workforce member or agent if reasonable diligence had been exercised and is subject to an outside (60-day) limit, plans are best-served by exercising reasonable diligence to detect events that might be breaches and requiring their business associates to do so as well. A health plan that does this can reasonably rely on the date that an event actually becomes known in determining how quickly notification might be required, and can take a reasonable amount of time to complete a prompt investigation and analysis of whether an event requires notification.

To allow sufficient time to investigate and analyze breaches occurring in the course of a business associate's operations, it may be necessary for a health plan to specify a much shorter reporting deadline than allowed by the regulations. The breach notification regulations require business associates to report breaches without unreasonable delay and in no event later than 60 days after discovering a breach. If a business associate is the health plan's agent, however, the health plan is deemed to have discovered an incident – causing the time to provide breach notification to begin running—at the time that it is known (or with reasonable diligence would be known) to the business associate. To counter this, in addition to requiring earlier reporting of breaches, a health plan might also want to specify in its business associate contract that the business associate is not an agent. If the business associate is not an agent, then the health plan is deemed to have discovered a breach occurring in the business associate's operation at the time it is reported.

## PROVIDING NOTIFICATION

When required, breach notification must be written in plain language and must include to the extent possible:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
- 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
- Any steps individuals should take to protect themselves from potential harm resulting from the breach
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, website or postal address

The rules imply that multiple notices may be required if additional information becomes available after the initial notification.

## GROUP HEALTH PLAN RESPONSIBILITIES

The group health plan that an employer maintains is the covered entity that is responsible for providing breach notification. Because the employer generally is responsible for the health plan's compliance, the employer must either provide required notification or arrange for a third party (e.g., a TPA) to do so on behalf of the plan.

As explained earlier, the regulations make business associates responsible for reporting breaches that occur in the course of the business associates' operations. The regulations stipulate that the business associate's report must include as much of the information that is required for the notification (listed above) as possible. In addition, the business associate must provide, to the extent possible, the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, used or disclosed as a result of the breach.

Employers that expect TPAs and other business associates to provide notification directly to affected individuals, HHS, and, if required, media outlets, need to negotiate amendments to business associate contracts delegating those duties.

## WHO IS NOTIFIED AND HOW

Notification is required for each individual whose unsecured PHI has been (or is reasonably believed to have been) used or disclosed as a result of the breach. While electronic notification is theoretically possible, it requires advance agreement by each individual that has not been withdrawn. Therefore, most notification provided in connection with employer plans generally will be provided by first-class mail to the recipient's last known address. Since notification is required for each individual affected by the breach, it does not appear that a single notice will suffice for all members of a family. If an affected individual has died, notification is to be provided to the individual's personal representative or next of kin.

If a health plan is not able to provide notification to some individuals because it has no address for them or it learns through returned mail that contact information is out of date, the health plan is required to provide "substitute notice." If substitute notice is required for fewer than 10 affected individuals, the plan can provide notice to them by e-mail, telephone or other means reasonably calculated to reach the individuals. If substitute notice is required for 10 or more affected individuals, then it must be provided by a conspicuous posting for at least 90 days on the home page of the plan's website or by a conspicuous notice in major print or broadcast media in areas where the affected individuals likely reside. The posting or media notice must include a toll-free phone number to call for information on whether a specific individual's PHI is affected. The number must remain active for at least 90 days. In addition to individual notification, media notification (e.g., by press release) is required if a breach affects more than 500 individuals in one state or other jurisdiction such as a county or city.

An employer may wish to establish a website for each plan that is subject to the breach notification requirements so that the website posting option is available for providing substitute notice when the plan has inadequate contact information for 10 or more affected individuals. Website posting is not an alternative to providing media notification if a breach affects more than 500 individuals in one state or other smaller jurisdiction.

## NOTIFICATION TO HHS

In addition to the affected individuals, HHS must be notified if a breach occurs with respect to unsecured PHI. If the breach involves 500 or more individuals (regardless of where they live), notification is due to HHS at the same time as it is due to affected individuals. If fewer than 500 individuals are affected, the health plan must maintain documentation and provide notification to HHS within 60 days after the end of each calendar year. HHS has provided [a reporting facility on its website](#) that specifies how both the immediate and year-end notification is to be provided.

## THERE'S MORE HIPAA WHERE THAT CAME FROM...

In addition to the breach notification requirements, several other legislative changes have been made to HIPAA's administrative simplification requirements, including:

- **Restrictions on Use of Genetic Information.** Under recently issued proposed revisions to the HIPAA privacy rules, health plans will no longer be allowed to use or disclose genetic information for underwriting purposes. If finalized in their current form, these regulations will become effective 180 days later and will require most health plans to revise and reissue their notices of privacy practices within 60 days after that.

- **Direct Application to Business Associates.** Starting February 17, 2010, many of the HIPAA security rules and at least one privacy rule will be enforceable directly against business associates, making them subject to HIPAA's civil and criminal penalties. Currently, business associates' security and privacy obligations are contractual obligations to health plans and other covered entities that are subject to HIPAA.
- **Restriction Requests.** Health plans and other covered entities must have procedures for individuals to request restrictions on uses and disclosures of their PHI and, if a covered entity agrees to a request, it must honor that agreement. Currently there is no requirement to agree to any request, but starting February 17, 2010, such a request must be honored if it relates to disclosing PHI to a health plan regarding an item or service for which full payment has been made.
- **Electronic Health Records.** These are electronic records of health information that are "created, gathered, managed, and consulted by authorized health care clinicians and staff," and some new requirements will apply to them starting in 2011 at the earliest. It is unclear currently whether these changes will have any effect on employer-sponsored health plans.
- **Enhanced Penalties and Enforcement.** These changes do not alter the actions that employers and plans must take to comply with HIPAA, but they do potentially increase the cost of noncompliance.
  - **Increased Civil Penalties for Violations.** Effective February 17, 2009 (upon enactment), the monetary penalties that an employer-sponsored health plan may incur for HIPAA privacy and security violations increased significantly. The current \$100 per violation penalty increased to \$1,000 per violation if it was due to reasonable cause and not willful neglect. A violation due to willful neglect may result in a \$10,000 penalty, if the violation is corrected, and a \$50,000 penalty if uncorrected.
  - **Enforcement by State Attorneys General.** Effective February 17, 2009 (upon enactment), state attorneys general are authorized to enforce HIPAA, and recovery may include attorney's fees. Previously, only HHS could enforce HIPAA requirements.
  - **Recovery by Individuals.** Currently, HIPAA does not have any provisions for individuals who are injured by privacy or security violations to receive any compensation through an enforcement action. HHS is now required to issue a regulation by February 17, 2012 that provides for individuals to receive a percentage of any civil monetary penalty or monetary settlement collected with respect to a violation that affects them.
  - **Additional HHS Audits.** The financing for HHS' auditing program has been revised to make more funds available for audits. In addition, HHS is now required to audit compliance in some cases.

These and other HIPAA updates will be the subject of future Willis EB Alerts.

# KEY CONTACTS

## US BENEFITS OFFICE LOCATIONS

### NEW ENGLAND

**Auburn, ME**  
207 783 2211

**Bangor, ME**  
207 942 4671

**Boston, MA**  
617 557 7517

**Hartford, CT**  
860 756 7365

**Manchester, NH**  
603 627 9583

**Portland, ME**  
207 553 2131

**Shelton, CT**  
203 924 2994

### NORTHEAST

**Buffalo, NY**  
716 856 1100

**Cranford, NJ**  
908 931 3005

**Florham Park, NJ**  
973 410 4622

**Morristown, NJ**  
973 829 6374  
973 829 6465

**New York, NY**  
212 915 8802

**Norwalk, CT**  
203 523 0501

**Philadelphia, PA**  
610 260 4351

**Radnor, PA**  
610 254 7289

**Wilmington, DE**  
302 397 0171

### ATLANTIC

**Baltimore, MD**  
410 584 7528

**Bethesda, MD**  
301 581 4261

**Knoxville, TN**  
865 588 8101

**Memphis, TN**  
901 248 3103

**Nashville, TN**  
615 872 3716

**Norfolk, VA**  
757 628 2303

**Reston, VA**  
703 435 7078

**Richmond, VA**  
804 527 2343

**Rockville, MD**  
301 692 3025

### SOUTHEAST

**Atlanta, GA**  
404 224 5000

**Birmingham, AL**  
205 871 3300

**Charlotte, NC**  
704 344 4856

**Gainesville, FL**  
352 378 2511

**Greenville, SC**  
704 344 4856

**Jacksonville, FL**  
904 355 4600

**Marietta, GA**  
770 425 6700

**Miami, FL**  
305 421 6208

**Mobile, AL**  
251 544 0212

**Orlando, FL**  
352 378 2511

**Raleigh, NC**  
704 344 4856

**Savannah, GA**  
912 239 9047

**Tallahassee, FL**  
850 385 3636

**Tampa, FL**  
813 490 6808  
813 289 7996

**Vero Beach, FL**  
772 469 2842

### MIDWEST

**Appleton, WI**  
414 259 8837

**Chicago, IL**  
312 527 6482  
312 621 4843  
312 621 4704

**Cleveland, OH**  
216 357 5921

**Columbus, OH**  
614 326 4788

**East Lansing, MI**  
517 349 3226

**Grand Rapids, MI**

248 735 7249

**Green Bay, WI**

414 259 8837

**Milwaukee, WI**

414 203 5248

414 259 8837

**Minneapolis, MN**

763 302 7131

763 302 7209

**Moline, IL**

309 764 9666

**Pittsburgh, PA**

412 645 8537

412 586 3524

**Schaumburg, IL**

847 517 3469

**SOUTH CENTRAL****Amarillo, TX**

806 376 4761

**Austin, TX**

512 651 1660

**Dallas, TX**

972 715 2194

972 715 6272

**Denver, CO**

303 765 1564

303 773 1373

**Houston, TX**

281 584 1672

281 584 1676

713 625 1017

**McAllen, TX**

956 682 9423

**Mills, WY**

307 266 6568

**New Orleans, LA**

504 581 6151

**Oklahoma City, OK**

405 232 0651

**Overland Park, KS**

913 498 4423

913 339 0800, ext. 108

**San Antonio, TX**

210 979 7470

**Wichita, KS**

316 263 3211

**WESTERN****Aliso Viejo, CA**

949 461 3996

**Fresno, CA**

559 256 6212

**Las Vegas, NV**

602 787 6235

602 787 6078

**Los Angeles, CA**

213 607 6300

**Novato, CA**

415 493 5210

**Phoenix, AZ**

602 787 6235

602 787 6078

**Portland, OR**

503 274 6224

**Rancho/Irvine, CA**

562 435 2259

**San Diego, CA**

858 535 1800

858 678 2130

**San Francisco, CA**

415 291 1567

**San Jose, CA**

408 436 7000

**Seattle, WA**

800 456 1415

*The information contained in this publication is not intended to represent legal or tax advice and has been prepared solely for educational purposes. You may wish to consult your attorney or tax adviser regarding issues raised in this publication.*