



# **Current Issues in Health Information Privacy**

*Iowa HIMSS Chapter Meeting  
May 6, 2010*



# Topics

- HIPAA Enforcement Data
- Breach Notification Rule
- HIPAA Investigation Tips



# **HIPAA Enforcement Data**

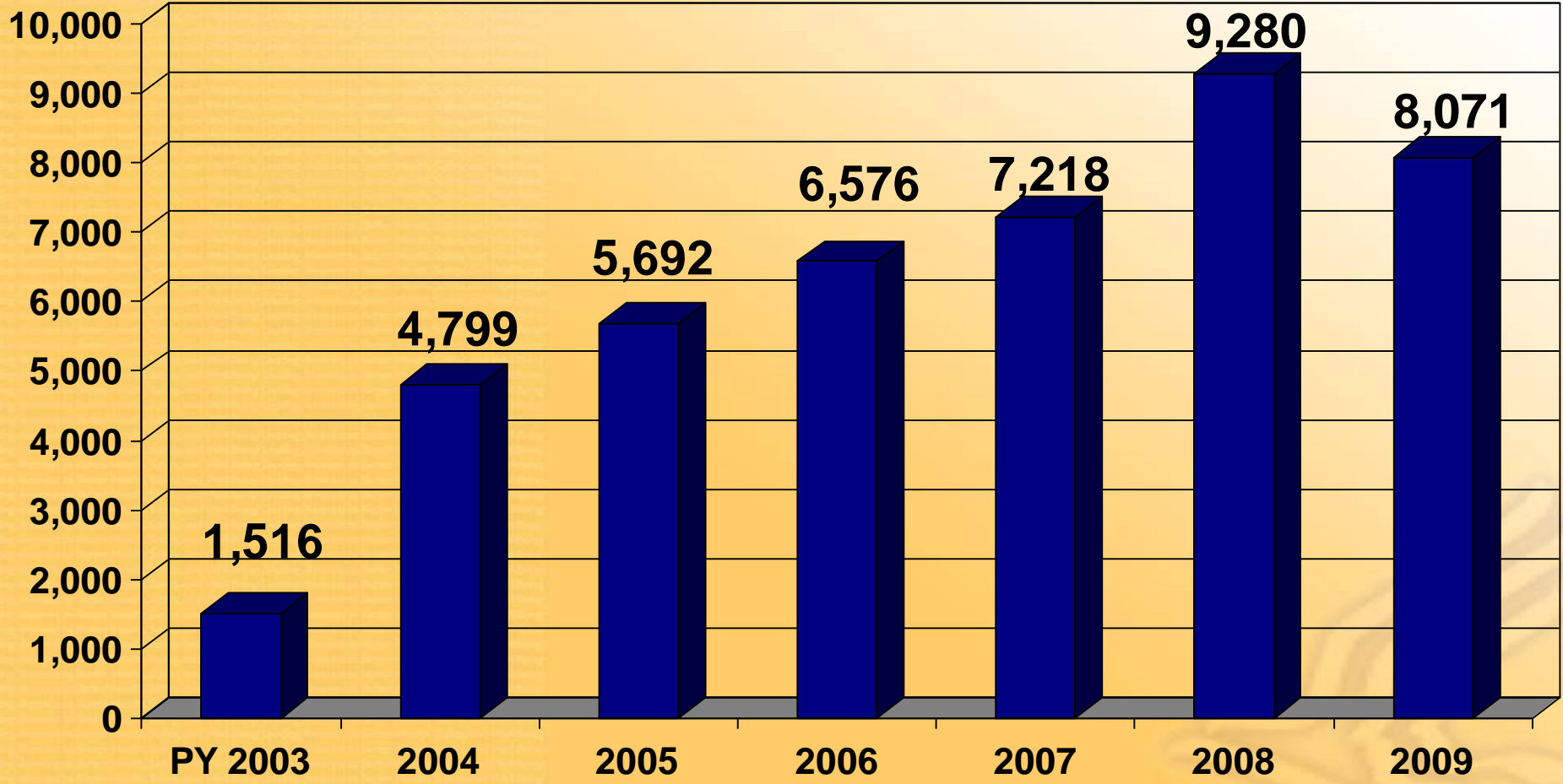


# Pie Chart: All Complaints





# Total Resolutions by Calendar Year





# Pie Chart: Total Investigated

## Total Investigated Resolutions

April 14, 2003 - March 31, 2010

Corrective Action Obtained  
(Change Achieved) (66%)

10,515

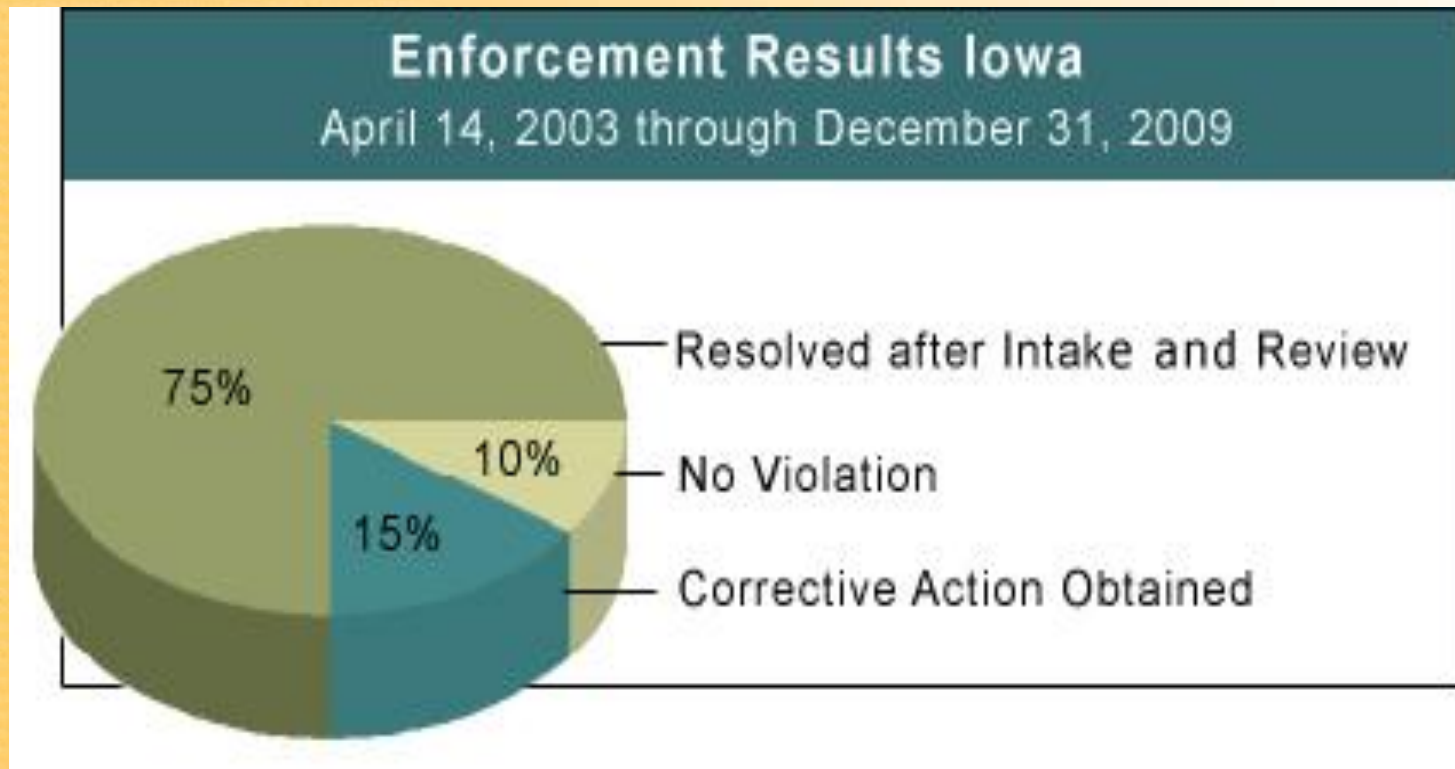
No Violation (34%)

5,462

**Total Complaints Investigated 15,977**



# Enforcement Results--Iowa





# Issues in Enforcement Actions

(April 14, 2003 to March 31, 2010 )

The compliance issues investigated most frequently, in order, are:

- Impermissible use or disclosure of an individual's identifiable health information
- The lack of adequate safeguards to protect identifiable health information
- Refusal or failure to provide the individual with access to or a copy of his/her records
- The use or disclosure of more than the minimally necessary protected health information
- Complaints to the covered entity.



# **Covered Entities in Enforcement Actions**

**(April 14, 2003 to March 31, 2010)**

The most common types of covered entities that have been required to take corrective actions and voluntarily comply, in order of frequency, are:

- Private physician practices
- General hospitals
- Outpatient facilities
- Health plans (Group Health Plans & Health Insurance Issuers)
- Pharmacies



United States Department of  
**Health & Human Services**

*Office of the Secretary*  
**Office for Civil Rights (OCR)**

# **Breach Notification Rule**



# Brief Summary

- **Covered entities must:**
  - **notify each affected individual of breach of “unsecured protected health information.”**
  - **Notice to media if more than 500 people in single area affected.**
  - **Notice to Secretary of breach through OCR website.**
  - **Most notifications must be provided without unreasonable delay (but no later than 60 days) of discovery of breach.**
- **Business associate must notify covered entity of breach and identify individuals affected.**
- **Effective date – September 23, 2009.**
- **No CMPs/sanctions imposed for failure to provide notification for 180 days after publication date for violations of Subpart D.**



# Breach Defined

- An impermissible acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.
- To compromise the security or privacy means to pose a *significant risk* of financial, reputational, or other harm to the individual.
- Uses or disclosures of limited data sets in which all dates of birth and zip codes have also been removed are not considered to compromise the security or privacy of PHI.

45 C.F.R. §164.402



# Significant Risk of Harm

- Determined by the covered entity through a risk assessment once it learns of a possible breach.
- In determining the level of risk, the covered entity should make a fact-based evaluation of factors such as the recipient of the PHI, the nature of PHI itself, any mitigation that can be taken to lessen potential harm, and the likelihood the PHI can readily identify an individual.

45 C.F.R. §164.402(1)(i)



# Breach Definition—Exceptions

1. Unintentional acquisition, access, or use of PHI by workforce member or person acting under the authority of a CE or BA if made in good faith and in the scope of authority and there is no further impermissible use or disclosure of the PHI.
2. Inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA or OHCA if the information received is not further impermissibly used or disclosed by the recipient.
3. CE or BA have a good faith reason to believe the unauthorized recipient of PHI could not reasonably have been able to retain the information.

45 C.F.R. §164.402(2)



# Notification obligation only applies to “Unsecured PHI”

- Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals per guidance issued by the Secretary and available on the OCR website (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>).
- Acceptable methods of securing PHI are encryption and destruction.
- Loss or compromise of PHI that has been encrypted or destroyed pursuant to the guidance does not trigger the duty to provide breach notification.



# Notification to Individuals

Following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of the breach.

45 C.F.R. §164.404(a)(1)



# Discovery of a Breach

- A breach is “discovered” by a CE on the first day the breach is known to the CE, or by exercising reasonable diligence, would have been known to the CE.
- Employees of a covered entity are considered agents of the organization and any knowledge an employee has will be attributed to the covered entity (except where the employee is the person committing the breach).
- Covered entities should have reasonable systems and procedures in place to discover breaches. This includes training staff on prompt reporting of any known breaches.

45 C.F.R. §164.404(a)(2)



# Time Lines for Individual Notification

- Breach notification must be provided to the individual without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach.
- 60 days is an outer limit, if the covered entity has completed its risk assessment and confirmed the breach within 20 days, it should send the notifications immediately instead of waiting until day 60.

45 C.F.R. §164.404(b)



# Notification Content

The notification must contain, to the extent possible, the following:

- A description of what happened and dates, if known
- A description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- A description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, e-mail address, website, or postal address
- The notification must be written in plain language.

45 C.F.R. §164.404(c)



# Methods of Individual Notification

- Written notice by first-class mail to last known address or by e-mail if agreed to by the individual.
- If the individual is deceased, notification may be sent to the next of kin or personal representative of the individual (if the CE knows the individual is deceased and has contact information for the next of kin or personal representative).
- Notification may be provided in one or more mailings as information becomes available.
- In urgent situations in which the CE believes there may be imminent misuse of unsecured PHI, notice may be provided to individuals by telephone or other means in addition to written notice.

45 C.F.R. §164.404(d)



# Substitute Individual Notification

Where there is insufficient or out-of-date contact information, a substitute form of individual notice reasonably calculated to reach the individual must be provided.

If the individual is deceased and there is insufficient contact information for the decedent's next of kin or personal representative, no substitute notification is required.

45 C.F.R. §164.404(d)



# **Substitute Individual Notification— Less Than 10 Persons**

If a CE determines that it has insufficient or out-of date contact information for less than 10 individuals affected by a breach, the CE may provide notification through:

- alternative form of written notice
- telephone notice
- other means

The substitute notice must include the same information as the written notice to individuals.

45 C.F.R. §164.404(d)(2)(i)



# Substitute Individual Notification— 10 Persons or More

If the covered entity does not have sufficient contact information for ten or more affected individuals, the following applies:

CE must post the notice conspicuously for 90 days on the home page of its website or provide the notice via print or broadcast media where individuals affected by the breach likely reside;  
**and**

CE must include a toll-free number that remains active for at least 90 days where individuals can learn whether they were affected by the breach.

The posting must include the same information as the written notice to individuals.

45 C.F.R. §164.404(d)(2)



# Media Notification

- For a breach involving more than 500 residents of a State or jurisdiction, the covered entity must notify prominent media outlets serving that State or jurisdiction in addition to written notice to individuals.
- Must be done without unreasonable delay, no later than 60 days after discovery of breach.
- Content of the notification to media is the same as that which must be provided to individuals.

45 C.F.R. §164.406



# Notification to the HHS Secretary

For breaches affecting 500 or more individuals, the covered entity must report the breach to the Secretary without unreasonable delay and not later than 60 days after discovery of the breach.

For breaches affecting fewer than 500 individuals, the covered entity may report the breach to the Secretary annually.

Reporting by covered entities will be done via OCR's website, at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.

This data is collected for reporting to Congress and notification to the Regions.

45 C.F.R. §164.408



# Business Associates

- Business associates must notify covered entities of breaches without unreasonable delay and in no case later than 60 days.
- Breaches are treated as discovered on the first day that the breach is known to the BA or by exercising reasonable diligence should have been known to the BA.
- The content of the notification from the BA to the CE must include, to the extent possible, the identification of the affected individuals and any other information that is known to the BA that the CE is required to include in its notice to the individual.

45 C.F.R. §164.410



## **CE/BA Relationship--Timing**

If the BA is an independent contractor of the CE, the CE discovers the breach upon receiving notification from the BA.

An example of an independent contractor BA is one in which the CE obtains a product or service, such as a transcription of medical records, but the CE does not have control over how the BA creates/performs the product or service.

If the BA is acting as an agent of the CE, the BA's knowledge of the breach is imputed to the CE. Therefore, the CE discovers the breach when the CE knew, or by exercising reasonable diligence, would have known, of the breach.



# Notification Delay for Law Enforcement

- If law enforcement gives a written statement to a CE or BA stating that the provision of the required notification would impede a criminal investigation, the CE or BA must delay notification until the time specified by law enforcement.
- If the requested delay by law enforcement is oral, the CE or BA must document the oral request and delay notification for no longer than 30 days from the date of the request.

45 C.F.R. §164.412



# Administrative Issues

- Many of the administrative requirements at section 164.530 incorporate the breach notification rules we've discussed.
- In the event of an impermissible use or disclosure of PHI, the covered entity or business associate has the burden of demonstrating that all notifications were made as required by the breach notification rules, or that the incident did not constitute a breach.

45 C.F.R. §164.414



## **Additional Information on the Internet**

### **OCR Breach Notification Rule Web Pages:**

[http://www.hhs.gov/ocr/privacy/hipaa/administrative/  
breachnotificationrule/index.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html)





# **HIPAA Investigation Tips**



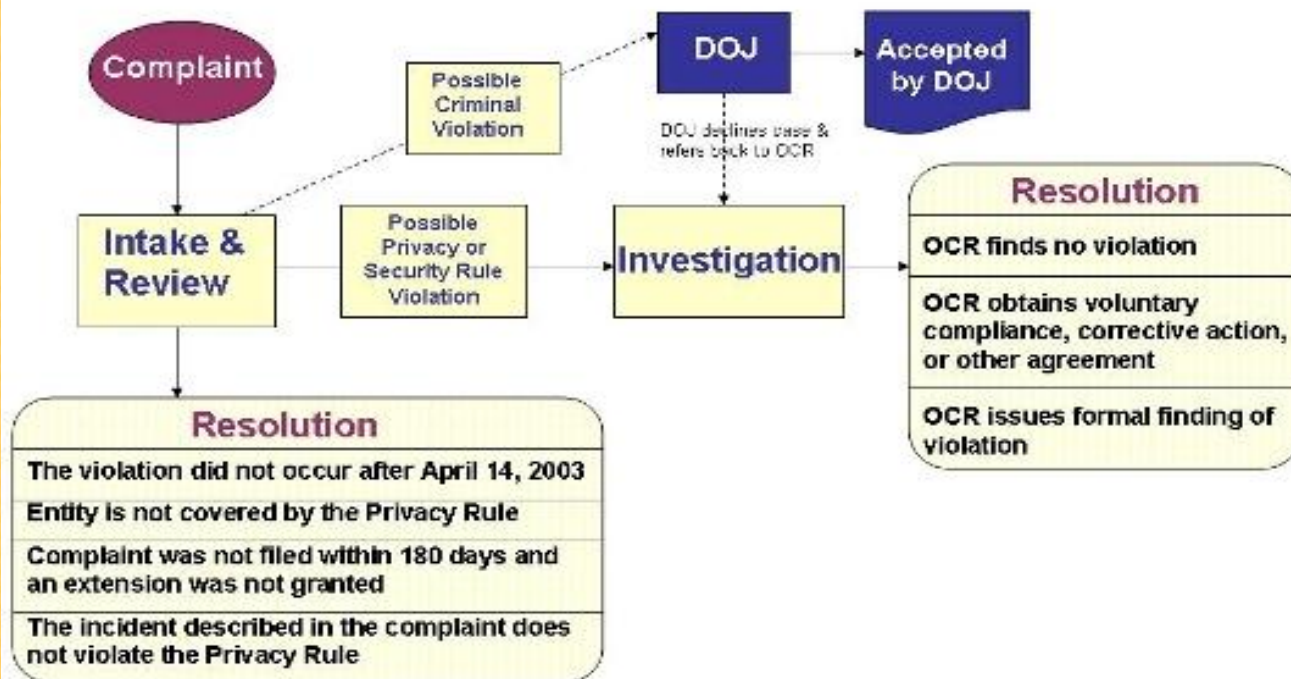
# Complaint Investigations

- Every complaint received by OCR is reviewed and allegations analyzed.
- An investigation is launched when warranted by the facts and circumstances presented by the complaint.
- OCR investigations have resulted in changes in privacy practices and other corrective actions in over 10,515 cases since April 2003.
- Corrective action obtained by HHS from covered entities has resulted in systemic change that benefits all individuals they serve.



# Enforcement Process

## HIPAA Privacy & Security Rule Complaint Process





# Civil Money Penalty Amounts

	<b>For violations occurring prior to 2/18/2009</b>	<b>For violations occurring on or after 2/18/2009</b>
<b>Penalty Amount</b>	<b>Up to \$100 per violation</b>	<b>\$100 to \$50,000 or more per violation</b>
<b>Calendar Year Cap</b>	<b>\$25,000</b>	<b>\$1,500,000</b>

•OCR may reduce a penalty if the failure to comply was due to reasonable cause and not willful neglect, and the penalty would be excessive relative to the noncompliance.



# Tips for CE Privacy Officers During an OCR Investigation

- When notification letter is received, contact investigator named in letter. Establish effective communication with investigator. Contact investigator for assistance with questions, such as, “How does this work...?”
- Respond within stated time frames. If CE cannot make the due date, let investigator know. Request a reasonable extension of time – enough so CE can accomplish the requested task. Avoid multiple requests for time extensions. Return telephone calls from the OCR investigator promptly.



# Investigation Tips (cont'd)

- If a CE is aware of a Privacy or Security Rule incident even before receiving the notification letter, start gathering relevant materials and facts. Formulate a corrective action plan (CAP) and execute it. An executed CAP will then be ready to deliver to the investigator when notification letter is received.
- Be specific in your responses to requests for data and information. For example, if training was provided, provide all the facts – when, who was trained (sign-in sheet), topics covered; if a policy has been revised, send a copy of the old policy and the new policy. Do not send entire privacy policies and procedures manual unless specifically requested.



# Investigation Tips (cont'd)

- Understand that investigations take place over an extended period of time. OCR investigator will work hard to be timely, but some investigations take longer than others.
- Be cooperative with the OCR investigator. Facts need to be confirmed by OCR. If OCR requests to interview an employee or requests contact information for former employees, provide this information in a timely manner. If you cannot, explain why.
- Ask for technical assistance if you do not understand what is expected by a particular requirement of the Privacy, Security or Breach Notification Rule.



# **Investigation Tips (cont'd)**

- Be forthcoming and acknowledge errors if they occurred. Remember, the goal is resolution through voluntary compliance and completed corrective action.
- Respond. Ignoring the investigation will exacerbate the matter.



# Investigation tips after HITECH

## PREVENT

- Become familiar with HIPAA compliance obligations
- Develop and implement compliant policies and procedures
- Train staff accordingly
- Invoke the Breach Notification safe harbor (properly secured e-phi)

## DETECT

- Bolster complaint process to resolve cases prior to federal involvement
- Provide for and respond to internal indications of non-compliance

## QUICKLY CORRECT

- Promptly address source, discontinue the violation
- Bring non-compliant policies and procedures into compliance
- Follow HIPAA-relevant remediation requirements



# **Our Mutual Goal**

Ensuring the privacy of each individual's health information in accordance with the standards and requirements of the Privacy, Security and Breach Notification Rules.





# Want More Information?

The OCR website, <http://www.hhs.gov/ocr/hipaa/>, offers a wide range of helpful information about the Privacy, Security and Breach Notification Rules:

- The full text of the Privacy, Security and Breach Notification Rules
- Privacy, Security and Breach Notification Rule summaries
- A covered entity "decision tool" to assist individuals and entities in making these determinations
- Over 200 frequently asked questions
- Fact sheets
- Information about the OCR enforcement program



# My Contact Information

Steven Mitchell

US Department of Health & Human Services

Office for Civil Rights

(816)426-7239

[steven.mitchell@hhs.gov](mailto:steven.mitchell@hhs.gov)