HIPAA Compliance Officer Training
By HITECH Compliance Associates

Building a “Culture of Compliance”

Your Instructor Is Michael McCoy
Nationally Recognized HIPAA Expert
Nothing contained herein should be considered to be legal advice. HITECH Compliance Associates is not an attorney firm and does not have attorneys on staff. All recommendations are from HHS, OCR, OIG and the guidelines set forth under HIPAA and the Omnibus Rule as reviewed by HITECH Compliance Associates’ professionals.
SUBJECTS COVERED
OCR Access Guidance
HIPAA Privacy Rule
HIPAA Security Rule
Ransomware
DHHS – Department of Health & Human Services  
CMS – Centers for Medicare and Medicaid Services  
OCR- Office for Civil Rights  
PII – Personally identifiable information  
TPO – Treatment, Payment, and Health Care Operations  
PHI – Protected Health Information  
ePHI – Electronic Protected Health Information  
Sensitive PHI (sPHI) – Special Class of PHI  
Malware – All Classes of Malicious Software  
Meaningful Use – EHR Requirements for Stimulus Funds  
Willful Neglect - Conscious, Intentional Failure or Reckless Indifference to the Obligation to Comply with HIPAA
Every Covered Entity Must Have A Responsible Person

HIPAA Security Officer
HIPAA Privacy Officer

Commonly known as the

HIPAA Compliance Officer

These are not just job titles, the position has responsibilities under federal law.
“HIPAA Obligations”

You have a

“Serious Responsibility”
Willful Neglect

Minimum Mandatory Fines. $25,000 to $5,550,000.

1. Not Performing **Risk Assessments** on a Regular Basis

2. Not Having a Complete Set of Policies and Procedures
   a. Privacy Rule
   b. Security Rule

3. Not **Training** Your Staff on Your Policies and Procedures
A Patient’s Right to Access

Major Provisions

1. Designated Record Set
2. Fees
3. Timeliness
4. Format
5. Email
6. Direct to 3rd Party
7. Access Directly
A covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access. For example, a doctor may not require an individual:

1) Who wants a copy of her medical record mailed to her home address to physically come to the doctor’s office to request access and provide proof of identity in person.

2) To use a web portal for requesting access, as not all individuals will have ready access to the portal.

3) To mail an access request, as this would unreasonably delay the covered entity’s receipt of the request and thus, the individual’s access.
Updated Guidance

Fees:
1) $6.50 Flat Fee
2) Actual Costs
3) Average Costs

OCR says have your cost documentation. You must provide upon request.
Fees:

The fee **may not include** costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above **even if** such costs are authorized by State law.
Fees:

DO NOT CHARGE FOR MEDICAL RECORDS UNTIL YOUR RATES ARE POSTED (Web or Lobby).

Covered entity must inform the individual in advance of the approximate fee that may be charged for copies of the PHI. This includes disclosure of costs for both paper and electronic records.
Updated Guidance

Authorizations Vs. Access

Is the patient the responsible party? – Access Request.

Nobody Knows. Be Safe.
Format

You Are Required to Provide All Formats That You Can Readily Produce.

Thumb Drive, CD
Updated Guidance

Emailing of PHI

You Must Email Records Upon Request

Protections must be in place and documented.

Using secure email to patients will cost you time.
Updated Guidance

Patient Can Direct to Any 3rd Party

Get Signed Documentation.

Do Not Treat a Request for Access as an Authorization, even if the Request Comes Authorization Form.
Patient Can Direct to An App

You Must Send to 3rd Party Apps If You Have the Capability.
Updated Guidance

Access Directly

Patients Have a HIPAA Right to Access their PHI As It Is Maintained in Your Electronic Medical Records and Practice Management System.

Set Up A Station For Viewing Medical Records.

Patient Is Allowed To Take Photos of Screens.

No Fees or Charges Allowed.
Cannot Require Patient To Use Portal That Could Create A Burden.
Compliance Is A Process

8 Steps to HIPAA Compliance
STEP 1 – Risk Management

Risk Assessment & Risk Management Plan

Performed Yearly to verify that Reasonable and Appropriate Security Measures are in Place.
STEP 1 – Risk Management

Risk Assessment & Risk Management Plan

Best if Performed by Qualified Professional
Could be IT Vendor, but Not the Best Idea

Save Time, Money and Get A Better Understanding of Risks.
Definition of a Business Associate as Updated by the Omnibus Rule

The Omnibus Rule amends the definition of a “business associate” to mean a person or entity that creates, receives, maintains or transmits protected health information to perform certain functions or activities on behalf of a covered entity.

Business associates cannot avoid regulatory liability or limit that liability by refusing to sign a Business Associate Agreement. In addition, business associates must ensure that any subcontractors who handle PHI also have a business associate agreement in place. A business associate agreement of a subcontractor is not required to be in place with the covered entity, only the business associate.
Keep a List of All Business Associates

Common Business Associates. **Vendors who routinely access PHI i.e. vendor that gets authorizations**, IT Vendor, Answering Service, Billing Company, Clearinghouse, Transcription Service, Off-Site Record Storage & Retrieval, Record Disposal Service, Shredding Company, Marketing Companies, Consultants, Practice Management Vendors, Electronic Medical Record Software Vendor, Equipment Maintenance & Repair, IT Hardware Vendors, Courier Service, Lawyers, Copier Company, Translation Services, Collection Agencies and others who have access to your ePHI or computer network.

Not Business Associates: Cleaning staff, lawyers and accountants that do not receive patient information (PHI).
It is a HIPAA violation, “Impermissible Disclosure” for a Covered Entity to have a Business Associate without a Business Associate Agreement.

Average Fine For No BAA - $1,800,000
STEP 2 – Business Associates

Business Associate Agreements Are Required

List of Business Associates – See OCR Requested Data on BAs

Due Diligence – Are You Giving PHI to a Non-Compliant BA

Oversight – How are you Maintaining Oversight of PHI by the BA
Cloud Guidance

When a covered entity engages the services of a CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate under HIPAA. Further, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data.
Cloud Guidance

You Need To Have a

**Service Level Agreement to Define**

- System availability and reliability:

- Back-up and data recovery (e.g., as necessary to be able to respond to a ransomware attack or other emergency situation):

- Manner in which data will be returned to the customer after service use termination (must be in user readable format):

- Type of Encryption used for data-at-rest: (include Key Management process)

- Type of Encryption used for data-in-transit: (include Key Management process)
Cloud Computing

Service Level Agreement should include:

No “Data Blocking”
Availability
Backup – Disaster Recovery
Security Controls
Accounting of Disclosures
Return or Destroy
Cloud Computing

You Do Not Have A Backup Of Your Patient Data
Policies and Procedures

- Privacy Rule
- Security Rule
- Breach Notification Rule
- Section 1557
Privacy Rule

Patient’s Privacy Rights
1. Right to Access.
2. Right to Request to Amend.
3. Right to Confidential Communications.
4. Right to Accounting of Disclosures.
5. Right to Restrict Information.
(Patients must resign Acknowledgement every 3 years)
Right to File A Complaint.

Most Common Reason for OCR Investigation – Privacy Right Violated.
The Minimum Necessary Standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule’s requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.
Authorization Form
Medical Records Release Form
Nine Elements Required by HIPAA

Authorization to Use and/or Disclose Medical Records

I give authorization to the provider listed below to disclose a copy of the specific health information identified below:

NAME OF PATIENT

DOB

<table>
<thead>
<tr>
<th>RECORDS FROM</th>
<th>Who is Releasing the Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Phone</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>City/State/Zip</td>
<td></td>
</tr>
</tbody>
</table>

For the Following Purpose:

- Personal Information
- Legal Follow-up
- Other...

Be Checking the Boxes Below, I Specifically Authorize the Use and/or Disclosure of the Following Health Information and/or Medical Records, If Such Information and/or Records Exist:

- Office Notes and Reports
- Mental Health Information and/or Records
- Other...

The Following Items Must Be Included to be Included in the Use and/or Disclosure:

- HIV/AIDS-related information
- Mental Health Information
- Drug/Alcohol Diagnosis

I understand that, if I am not authorized to receive the information, it is not a health care provider or health plan covered by federal privacy regulations, the information described above may be re-disclosed and no longer protected by HIPAA and other federal and state regulations. However, the recipient may be prohibited from disclosing these health information under the Federal Substance Abuse Confidentiality Requirements.

I further understand that the person or entity receiving the information may not re-disclose or further re-disclose the information without my consent.

I understand that re-disclosure of the information may not affect the recipient's liability for re-disclosure if the re-disclosure is to a recipient that is subject to the Privacy Rule. I further understand that a limitation will not affect the person or entity's ability to re-disclose information in reliance on the authorization form.

I understand that the provider may not condition treatment on the patient signing the authorization form.

I further understand that, if the use or disclosure is for research-related treatment or PR (created for use by a third party),

Print Patient’s Name: ____________________________
Signature of Patient or Patient's Legal Representative: ____________________________
Print Name of Legal Representative (if applicable): ____________________________
Relationship to patient: ____________________________

Date: ____________________________

Description of the information to be used or disclosed:

A description of each purpose of the requested use or disclosure, including a specific statement at the request of the individual is a sufficient description of the purpose when an individual initiates the authorization.

Name or other specific identification of the person or class of persons authorized to make the requested use or disclosure:

Name or other specific identification of the person or class of persons authorized to make the requested use or disclosure.

Expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure:

States that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the Privacy Rule.

Signature of Individual and Date: ____________________________
Subpoenas

Must Have Signed Valid Authorization

Or

Notice of Production (HIPAA Release)

HIPAA does not allow release of PHI with only a Subpoena
Permitted Disclosures

HIPAA provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities without first obtaining an individual’s authorization: including for treatment, payment and for health care operations.
## HIPAA Security Rule

### The Security Matrix

#### Step 3 – Policies & Procedures

<table>
<thead>
<tr>
<th>Security Standards Matrix (Appendix A of the Security Rule)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrative Safeguards</strong></td>
</tr>
<tr>
<td>Standards</td>
</tr>
<tr>
<td>Security Management Policies</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

#### PHYSICAL SAFEGUARDS

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications (If Required) (If Applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>§ 164.308(a)(1)</td>
<td>Risk Analysis (A)</td>
</tr>
<tr>
<td>Controls</td>
<td></td>
<td>Risk Management Policies (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Policy (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information System Audit Policy (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incidence Notification (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business Associate Contracts and Other Arrangements (A)</td>
</tr>
</tbody>
</table>

- **Compliance**
- **Regulations**
- **Guidelines**
HIPAA Training

- Yearly to **Your** Policies and Procedures
- General Training is not Sufficient.

- Before Access is Given to PHI
- Updates Throughout the Year.
- Document
Breach Notification Rule

Staff Need to be Able to Identify Breach

Breach Security Risk Assessment Must be Performed

Suspected Breach is Actual Breach.

Breach Reporting to OCR Portal (at end of year)
Small Breaches
500 or More - Immediately
Plan In Place for Breaches of Under 500 Records.

Plan In Place for Breaches of 500 or More Records.
  Breach Costs can be Staggering Even without Fines.
  Determining if a Breach Occurred Can Cost Thousands.
Breach Notification Plan

HIPAA Breaches Must Be Reported to the Patient

State Laws May Increase Your Breach Notification Requirements
Contingency Plan

How will you access your patient records in an emergency?

How fast can you restore from backup?

How old is your backup? Day, week, hour.
If it’s not documented, it’s not done.

STEP 7 – Documentation
STEP 7 – Documentation

Documentation is Key to Proving HIPAA Compliance

Mobile Device Policy

Patient Forms to Invoke their HIPAA Rights

Letters to Respond to HIPAA Requests

Certification of Proper Disposal of Systems Containing PHI

Job Descriptions

Visitor Sign-In Sheets
Required Postings

Last Year’s Audits Showed Up to 94% Failure to Comply

**Lobby**
Post Notice of Privacy Practices
Non-Discrimination Notice (Section 1557)
Pricing for Medical Records (if not posted on web site)

**Web Site – Must be Prominent and Downloadable**
Privacy Policy of Web Site
Notice of Privacy Practices
Pricing for Medical Records
Non-Discrimination
All HIPAA documentation must be kept for a period of 6 years.
System Activity Review
(User Audit Log)

User Audit Logs Must Be Reviewed & Documented

Use and Disclosure Tracked = Fax Machine, Firewall Penetration Reports, etc...

Monthly Activity
Your HIPAA Homework

Looking for Unusual or Suspicious Activity

May be the only way to detect an Insider Threat, Hacking and/or Other Improper Access and Use of Patient Records.
STEP 8 – System Activity Review

System Activity Review

Review Workforce Members for:
Number of Records Accessed
Location of Access
Time in Chart
Activity – Modified, downloaded, Viewed...

“HIPAA Homework”

Each Workforce Member Should Be Reviewed Twice Per Year Minimum

Audit Log Management Report

My Medical Practice  HIPAA Security Officer: Michael McCoy
Beginning Period of Review: 2/1/2015
Ending Period of Review: 2/20/2015

Audit Log was Stored in System
Audit Log was Attached

PURPOSE: To protect against threats or hazards to the security of the information and to preserve for investigations on potential security breaches our organization’s access system audit log on a routine basis. This report is the responsibility of the HIPAA Security Officer.

User Audit Log Reviewed

<table>
<thead>
<tr>
<th>USER ID 1</th>
<th>USER ID 2</th>
<th>USER ID 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time: 01/23</td>
<td>Holy416</td>
<td>Kathy89</td>
</tr>
<tr>
<td>02/20/2016</td>
<td>2/10/2016</td>
<td>3/4/2015</td>
</tr>
</tbody>
</table>

Activity: Viewed, Modified, Created, Time in Chart, Inappropriate Access, Access Same Last Name, Location of Access, Login Success/Failure

Patient Charts Reviewed

<table>
<thead>
<tr>
<th>PATIENT ID 1</th>
<th>PATIENT ID 2</th>
<th>PATIENT ID 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>234567</td>
<td>345678</td>
</tr>
<tr>
<td>2/13/2015</td>
<td>2/14/2015</td>
<td>2/17/2015</td>
</tr>
</tbody>
</table>

Activity: Viewed, Modified, Created, Time in Chart, Inappropriate Access, Access Same Last Name, Location of Access, Login Success/Failure

Results of Audit Log Review

Findings for this Period: The following items require investigation:

Investigations Required
- Staff member stated that another employee forgot their User ID and Password so they shared her User ID for the day. Verified that the other employee had no activity for the day and gave both employees a Group 1 Session.

- All findings that require additional investigation will be documented with a Security Incident Report.

Reviewed By: Michael D. McCoy
Title: HIPAA Security Officer
System Activity Review

Log-in Success and Failures to the Network also need to be reviewed.

Review Server and Workstation Event Logs for unusual and/or suspicious activity.
Build a Culture of Compliance

- Monthly System Activity Review Report
- Sanctions Given to Workforce Members
- Breach Security Risk Assessments
- Breach Reporting to OCR
- On-Going Staff Training

If it’s not documented, it’s not done.
Encryption of Email With PHI

REQUIRED. PERIOD.

Email from provider to provider.

Emailing within your practice.

Patient sends an email message to doctor.

Why does the hospital send my doctor unencrypted email with PHI?
Text Messaging of PHI

**REQUIRED.**

- Mobile Device Policy In Place and Signed.
- Deletion of Text Message When No Longer Needed.
- Even with “code” or short messages, protections must be in place.
Encryption Must Be Documented

- Screen Shots of Encryption In Use.
- Review of Encryption Method Used.
- Key Management Process.
Mobile Devices

Texting

Texting PHI — The Problem — Going to Happen

Policy to Mitigate Risk
Delete after use.
Reduce PHI disclosed.
Encrypt Device with 6 digit PIN or biometric.
“Code is Going to Protect the Practice”
Mobile Device Protections

Health IT.gov
1. Install and enable encryption to protect health information stored or sent by mobile devices.

2. Use a password or other user authentication.

3. Install and activate wiping and/or remote disabling to erase the data on your mobile device if it is lost or stolen.

4. Disable and do not install or use filesharing applications.

5. Install and enable a firewall to block unauthorized access.

6. Install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks.
Mobile Device Protections

7. Keep your security app up to date.

8. Research mobile applications (apps) before downloading.

9. Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use.

10. Use adequate security to send or receive health information over public Wi-Fi networks.

11. Delete all stored health information on your mobile device before discarding it.

12. Keep the OS up-to-date.
The Real Cost of HIPAA Violations

Loss of Trust Between You and Your Patients

Loss of Reputation.
"We ask for a lot of documentation because the law requires it."

Iliana Peters: Health Information Privacy Specialist
Office for Civil Rights
U.S. Department of Health & Human Services
JIGSAW RANSOMWARE

Your computer files have been encrypted. Your photos, videos, documents, etc.... But, don't worry! I have not deleted them, yet. You have 24 hours to pay 150 USD in Bitcoins to get the decryption key. Every hour files will be deleted. Increasing in amount every time. After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins. Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one. Send to the Bitcoins address specified. Within two minutes of receiving your payment your computer will receive the decryption key and return. Try anything funny and the computer has several safety measures to delete your files. As soon as the payment is received the crypted files will be returned to normal.

Thank you
Ransomware:
A Breach of Confidentiality, Integrity and Availability is Presumed.

Breach Risk Assessment to Perform LoProCo.
Low Probability that the PHI has been compromised.

Confidentiality – has PHI been accessed?
Integrity – most strains of ransomware copy files to encrypted container.
Availability – Loss of access to your PHI
Ransomware Is A Breach of PHI

A Breach Risk Assessment Must Be Performed.
Items to document include:

- Variant of the Ransomware
- Number of Patient Records Affected
- **Network Activity**
- Did the Malware Communicate with the Attacker
- Number of Days In the System
- A Network Activity Review
- Review for Other Malware such as Backdoors
- Data Integrity Checks
- Reasonable Security Measures in Place
- Boot Drive Locked or Files Locked
- Backdoors or Other Malware Present
Ransomware Is A Breach of PHI

Make Sure Your Office Has Essential Documentation Available.

Audit Logs Critical.
Network Activity.
Evidence of Malware Communication with Attacker.
Staff Training on Malware.
Ransomware:
The Stakes Are Higher, Pay or We Will Release Your Patient’s Information Onto the Internet

Tampa Bay Surgery Center sent a letter to 25,000 patients alerting them that their personal information was stolen last month and posted on a Twitter account used by the hacker group “The Dark Overlord.”

The Dark Overlord Gang stated in a press release that “Tampa Bay Surgery Center annoyed us” and that was the reason for the posting of PII.
Training and Awareness are Key
Increase Your IT Defenses

Ransomware Defenses

Data is categorized based on organization value. Implement physical and logical separation of network and data for different organizational units.

Penetration Tests are performed and remediated. Test the protection of your firewall.

Vulnerability Scans are performed and remediated. Uncover known vulnerabilities and other security concerns.

Bitcoin Account in Place or Accessible. Cybercriminals are likely to demand payment in Bitcoin. Bitcoin accounts can take days to set up.

Cyber Insurance in Place – Breach investigation and response can easily reach $100,000 or more.

Workstations are scanned for phishing. You may not know if workstations have 7hp. Use specialized software to search and secure your 7hp from your workstations.

Use 7hp software to monitor the computer and internet activity of your workforce. Software such as 7hp can monitor, record, and report your staff’s activity on the workstations and the internet.

Disable USB ports for mass storage devices. This will keep USB ports from being able to upload or download data. However, there will be the port open for printers, etc.

Put a password on the 7hp and restrict dual-booting of computers. This will keep the computing device from being altered in other than a normal device.

Use a password checking program to ensure all passwords used on the computing device meet “complex” criteria. This will check to ensure workforce members are keeping required security on all accounts and entries.

Disable Windows Script Host. Cybercriminals use to install malicious payloads.

Disable Windows PowerShell. Cybercriminals use to install malicious payloads.

Turn off unused Windows Connections and Implement MAC Address Filtering. Reduce entry points on your network.

Patch Web Browsers used on all computing devices. Patch known vulnerabilities.

Black known malicious 7hp Address. Have it update on a regular basis.

Close and monitor all unused ports. Restrict entry points on your network.

Black unnecessary outbound internet traffic or restrict internet traffic after work hours. Ransomware and other malware will want to communicate with the attacker. Block this communication.

Disable Micro and Macros, especially from Microsoft products. Macros are a common method of launching malware on your network.

If Mobile Devices are Connected to the Network, require user to only download apps from official store. Apps that have not been tested or reviewed may be unsafe.

Ensure staff is trained to not click on attachments with the following extensions. .exe, .pdf, .doc, .zip, .bat, .rar

Review Remote Desktop Protocol (RDP) also known as Remote Desktop Connection. If not used, disable. RDP connections are used as entry points by cybercriminals.

Use Secure Software to detect files that contain 7hp. Files deleted using the trash bin could still be available to cybercriminals.
Reporting Breaches to OCR
- Less than 500 Records -

Self-Report in January and February for Previous Year
Do You Have A Reportable Breach?

Under the breach notification rule, covered entities are only required to self-report if there is a "breach" of "unsecured" PHI. 45 CFR § 164.400

"Unsecured" PHI

is that which is "not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology" specified in HHS guidance. (45 CFR § 164.402). There are only two ways to "secure" PHI:

1. In the case of electronic PHI, by encryption that satisfies HHS standards; or
2. in the case of e-PHI or PHI maintained in hard copy form, by its complete destruction. (74 FR 42742).
Breach.

The unauthorized "acquisition, access, use, or disclosure" of unsecured PHI in violation of the HIPAA Privacy Rule is presumed to be a reportable breach unless the covered entity or business associate determines that there is a low probability that the data has been compromised or the action fits within an exception. (45 CFR § 164.402; see 78 FR 5641).
Notice to HHS.

Breaches of unsecured PHI must also be reported to HHS: breach reports involving more than 500 or more persons must be made within 60 days (30 days in Florida); breaches involving less than 500 must be reported within 60 days after the end of the calendar year. Covered entities submit the report electronically using the form available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
Full HIPAA Services Offered
Risk Assessment
Policies and Procedures
Training
HIPAA Security Officer Certification
Breach/Ransomware Consulting

www.HipaaComplianceKit.com
mm@HipaaComplianceKit.com
813-892-4411