



National Organization of Alternative Programs
2014 NOAP Educational Conference

HIPAA and Privacy Risks


Ira J Rothman, CPHIMS, CIPP/US/IT/E/G
Senior Vice President - Privacy Official

March 26, 2014



Learning Objectives

1. Understand US privacy law environment
2. Understand the applicability of HIPAA and other laws to the Alternative Programs
3. Discuss actions you should take to protect privacy



MAXIMUS 2 Helping Government Serve the People®

What is Privacy?

Privacy means being able to have control over how your information is collected, used, or shared;

Keeping your business to yourself

↓

Oftentimes laws, regulations and project contracts tell us what needs to be protected and to what level.

MAXIMUS 3 Helping Government Serve the People®

US Privacy Law Environment

Privacy in the United States is sectoral in nature.

There are different laws -- and different agencies responsible for those laws -- for different industry sectors. Here are some examples:

- Health Information
- Alcohol and Drug Abuse Patient Records
- Financial Information
- Marketing
- Law Enforcement
- Human Resources/Employment
- Department of Motor Vehicles
- Credit Reports
- Video Rental Information

There can be Federal Laws, State Laws and even Local laws all for the same industry sector.

MAXIMUS 4 Helping Government Serve the People®

What Laws Apply to You?

KNOW THE RULES!

Questions to ask:

- What information are you handling?
- Who is your client? What laws apply to them?
- What does your contract say the rules are?

MAXIMUS 5 Helping Government Serve the People®

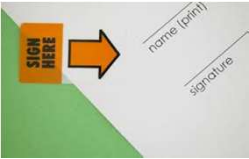
Confidentiality of Alcohol and Drug Abuse Patient Records Act of 1972

- Federal Law (implementing regulations - 42 CFR Part 2)
- Applies to any individual or entity that is federally assisted and holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment
 - ✓ Most drug and alcohol treatment programs are federally assisted.
- Special privacy protections for alcohol and drug abuse patient records
 - ✓ Information that identifies an individual directly or indirectly as having a current or past drug or alcohol problem, or as a participant in a covered program is covered.

MAXIMUS 6 Helping Government Serve the People®

Confidentiality of Alcohol and Drug Abuse Patient Records Act of 1972

- With limited exceptions, 42 CFR Part 2 requires **patient consent** for disclosures of protected health information even for the purposes of treatment, payment, or health care operations.
- Consent for disclosure must be in **writing**.



MAXIMUS 7 Helping Government Serve the People®

What is HIPAA?

Healthcare Insurance Portability and Accountability Act of 1996


HIPAA
Applies to entities who create, receive, maintain or transmit Protected Health Information.

- Covered Entity (CE)**
Health Plan, a Health Care Provider or a Health Care Clearinghouse that create certain transactions in electronic form.
- Business Associate (BA)**
A Business Associate (BA) provides functions, services, or activities by or on behalf of Covered Entities. The functions, services or activities involve the creation, receipt, maintenance or transmission of Protected Health Information. Merely maintaining PHI can trigger a BA relationship.

MAXIMUS 8 Helping Government Serve the People®


What is Protected Health Information (PHI)?

- Past, present, or future health or condition of an individual.
- Provision of healthcare to an individual.
- Payment for the provision of healthcare to an individual.
- Identifies or can be used to identify an individual.



MAXIMUS 9 Helping Government Serve the People®

Examples of PHI




- Name
- Address
- Email address
- Date of Birth
- Telephone or Fax Numbers
- Social Security Number
- Health Plan Enrollment Information

MAXIMUS 10 Helping Government Serve the People®

What is Personally Identifiable Information (PII)?


Personally Identifiable Information (PII) often refers to any information that can be used to identify or is associated with an individual.



MAXIMUS 11 Helping Government Serve the People®

Examples of PII


- Name
- Social Security Number
- Driver's License number
- Account Number, Credit or Debit Card Number, Other Financial Information
- Professional License Number
- Sometimes Health or Medical Information



The specific definition varies by state statute and project contracts

MAXIMUS 12 Helping Government Serve the People®

HIPAA Rules



- 1. Privacy Rule** – only use or disclose PHI to those who need to know it; use only the minimum necessary amount of information to complete the task at hand
- 2. Security Rule** – use reasonable and appropriate administrative, technical and physical safeguards to protect and secure PHI
- 3. Enforcement Rule** – penalties range from \$100 to \$1.5 million for each identical violation in a calendar year. There are four tiers of penalties.
- 4. Breach Notification Rule** – notify individuals, HHS and maybe the media if PHI is used by or disclosed to the wrong person

MAXIMUS 13 Helping Government Serve the People®

Enforcement Rule – Civil Money Penalties

Violation Category	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
Did Not Know [CE/BA did not know, and by exercising reasonable diligence, would not have known of the violation]	\$100 - \$50,000	\$1,500,000
Reasonable Cause [in between “did not know” and willful neglect]	\$1,000 - \$50,000	\$1,500,000
Willful Neglect - Corrected	\$10,000 - \$50,000	\$1,500,000
Willful Neglect – Not Corrected	\$50,000	\$1,500,000

MAXIMUS 14 Helping Government Serve the People®

What is an Incident?

An incident involves an unauthorized use or disclosure of PHI or PII that violates either Federal Laws, State Laws, Local Laws, your contract, or project policy.

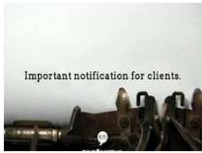
Bottom line: We did not keep information private.

MAXIMUS 15 Helping Government Serve the People®

Breach Notification Rule: Guilty Until Proven Innocent

When do you need to make a breach notification?

When there is anything greater than a “low probability that the protected health information has been compromised based on a risk assessment.”



• **The Federal Government assumes there is a breach unless you can determine there is a low probability that the data was compromised**

MAXIMUS 16 Helping Government Serve the People®

Determining the Probability the PHI is Compromised

An incident rises to the level of a breach if there is anything greater than a low probability that the PHI is compromised following an impermissible use or disclosure.

↓

HHS gave us four factors to consider when determining the probability.

↓

HHS requires us to conduct a thorough, good faith risk assessment using the four factors and to arrive at a reasonable conclusion.

MAXIMUS 17 Helping Government Serve the People®

The Four Factors 1 2 3 4

What is the nature and extent of the PHI involved?

- ✓ Types of identifiers and
- ✓ Likelihood of re-identification

- Name – full name? initials?
- Address
- Email address
- Date of Birth
- Telephone or Fax Numbers
- Social Security Number or HIC #? – redacted?
- Health Plan Enrollment Information
- Medical Records or History – how much information?

MAXIMUS 18 Helping Government Serve the People®

The Four Factors 1 2 3 4

Who was the unauthorized person who used the PHI or to whom the disclosure was made?

- An entity required to protect and secure the information?
- Another entity required to comply with HIPAA?
- Trusted entity?
- Unknown?
- Is there an ability to identify the individual whose PHI has been disclosed?

MAXIMUS 19 Helping Government Serve the People®

The Four Factors 1 2 3 4

Whether the PHI was actually acquired or viewed?

- Did the conversation take place?
- Was the envelope opened?
- What does forensic analysis of the laptop show?
- Was the email received?

MAXIMUS 20 Helping Government Serve the People®

The Four Factors 1 2 3 4

Extent to which the risk of PHI compromise has been mitigated?

- PHI is returned to MAXIMUS
- *Obtain assurance from the recipient that the PHI is securely destroyed
- *Obtain assurance from the recipient they will not further distribute the PHI
- Notify the affected individual
- Offer credit monitoring

MAXIMUS 21 Helping Government Serve the People®

There are three exceptions to a breach

A breach is, generally, the unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the security or privacy of the PHI. There are three exceptions.

A worker, in good faith, unintentionally acquires, accesses or uses PHI he was not supposed to and does not further use or disclose the PHI in an unpermitted way.	A worker at a CE or BA inadvertently receives information from a co-worker and does not do use or act upon the information in an unpermitted way.	We disclose PHI to an unauthorized person, but we have a good faith belief that the unauthorized person would not reasonably have been able to retain the information.
--	---	--

MAXIMUS 22 Helping Government Serve the People®

There is no breach if the PHI is secured

A breach is, generally, the unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the security or privacy of the PHI.

- Unsecured PHI is PHI that is not secured through the use of technology or methodology specified by the Secretary of Health and Human Services (HHS)
- Under the Guidance issued by the HHS Secretary, there are two ways to secure PHI (safe harbor):
 - ✓ Encrypt it (in specific ways required by HHS)
 - ✓ Destroy it (in specific ways required by HHS)
- There is **no breach** if the PHI has been **secured** or one of the three **exceptions** is met

MAXIMUS 23 Helping Government Serve the People®

Determining the Probability the PHI is Compromised

Step 1: Investigate and Determine Probability

- Nature and extent of the PHI involved
 - ✓ Types of identifiers and
 - ✓ Likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed and
- The extent to which the risk to the PHI has been mitigated

If the Probability is greater than a "low probability", start the notification process.

MAXIMUS 24 Helping Government Serve the People®

Breach Notification Process

Step 2:
Meet Notification Requirements

- Who do you need to notify?
- Affected individuals need to be notified by first class mail within 60 days


Step 3:
Write a Notice that Includes All the Required Elements

Step 4:
Depending on the number of individuals affected, notify the media and HHS

MAXIMUS 25 Helping Government Serve the People®

Scenario #1 – Sent information to the wrong Applicant

An Applicant (Applicant #1) calls the compliance monitor to inform her that the documents she received in the mail had someone else's name (Applicant #2) on them.



Is this an incident?

What do you do?

MAXIMUS 26 Helping Government Serve the People®

Scenario #1: Discussion

Incident?

- Disclosing (or sharing) information regarding an Applicant to anyone who does not need to know that information is a **privacy incident**.

Trust

- Individuals have a right to **EXPECT** and **TRUST** us to treat their personal information with the same care we would want others to treat our personal information. Who are we to disclose that information to the wrong person?

Required

- Federal law, State laws, and our contracts with our clients **REQUIRE** us to have safeguards in place to protect and secure protected health information and personally identifiable information. **Disclosing Applicant #2's information to Applicant #1 is a violation.**

MAXIMUS 27 Helping Government Serve the People®

Scenario #1: What do you do?

Investigate

- After researching, the project found that the worker responsible for quality checking the documents to ensure placement in the correct envelope failed to identify the error.
- The project contacted Applicant #2 who confirmed she received the correct documents.
- The project confirmed the data elements that were disclosed were limited to NAME


Mitigate

- The project sent Applicant #1 a prepaid FedEx envelope to facilitate the return of the document to the project
- The project resent Applicant #1 a correct set of documents

MAXIMUS 28 Helping Government Serve the People®

Breach Notification: State and Local Laws


- 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information
 - ✓ Usually SS# and Name
 - ✓ Usually computerized data



- State notification laws may be more restrictive


MAXIMUS 29 Helping Government Serve the People®

How Do Incidents Start?



MAXIMUS 30 Helping Government Serve the People®

Scenario #2: Email Woes




You need to email the project client a file containing information regarding Applicants. The file contains the names, addresses, and license numbers for the Applicants. You type in the email address, attach the file, and press send. Only after you press send do you realize that you selected your friend's email address instead of the client's email address.

What do you do?

MAXIMUS 31 Helping Government Serve the People®

Scenario #3: May I have your password, please?

"Technical Services" calls David and requests his password...




What should David do?

MAXIMUS 32 Helping Government Serve the People®

Stop. Think. Protect.

- ✓ Is the right letter or attachment in the right envelope?
- ✓ Is the person on the phone the right person?
- ✓ Is the mail or email going to the right person?
- ✓ Is there any PHI or PII in the email? If yes, is the PHI or PII needed? Is the email secure?
- ✓ Does something seem off? Double check it!




Your client's privacy is in your hands.....

MAXIMUS 33 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Training and Education

- Provide privacy and security training for all workers
- Ensure training is documented by a signed attendance sheet/log
- In the case of workers with access to PHI, training takes place prior to granting access
- Regularly educate staff regarding the privacy and security requirements with a focus on specific job responsibilities




MAXIMUS 34 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Physical security measures

- Have physical office controls (e.g., locked doors) in place to restrict access to authorized staff
- Do not allow someone access to a space using someone else's badge
- Question anyone without a badge



MAXIMUS 35 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Physical security measures

- Do not discuss PHI/PII where others can hear it. This includes office staff that do not have a need to hear the PHI/PII for their work
- Ensure workers lock computer screens every time they walk away from their desks, even if it is just for a minute. A minute is enough time for an unauthorized user to access a computer
- Require workers to log off their computer each night to allow anti-virus and operating system updates to run
- Do not leave PHI/PII in view on screen unnecessarily


CTRL-ALT-DEL

MAXIMUS 36 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Physical security measures

- Clear desks and secure PHI/PII when leaving the desk
- Situate desks so PHI/PII cannot be seen from the outside
- Locate fax machines in secure areas
- Remove PHI/PII from fax machines, printers, and copiers promptly
- If workers do not need to print PHI/PII to complete the task at hand, they should not print the PHI/PII
- Shred (or dispose of in a secure recycle bin) PHI/PII



MAXIMUS 37 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Policies and Procedures

- Develop and implement a Sanctions Policy
- Ensure privacy and security related policies and procedures are readily available for workers to review



MAXIMUS 38 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Passwords and Unique User IDs

- Use complex passwords (at least eight characters with upper and lower case letters, numbers, and symbols)

Example: J@A&m03!

- Assign anyone with the ability to view, receive, or modify PHI/PII a unique user ID

Example: JD54302

MAXIMUS 39 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Minimum necessary

- Use only the minimum necessary PHI/PII to complete the task at hand




MAXIMUS 40 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Email

- Do not send PHI/PII to anyone outside your email network – even a client – through email unless it is properly encrypted
- Never forward or send business related email to your personal email address
- Email that is not properly secured can be intercepted during transmission
- It's hard to determine where your email goes after it arrives in the recipient's inbox; where is it being forwarded?




MAXIMUS 41 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Laptops

- Do not leave laptops unattended while traveling. Never check laptops when checking in at the airport.
- All laptop hard drives should be encrypted per Federal specifications (valid encryption is a safe harbor for breach notification)




MAXIMUS 42 Helping Government Serve the People®

Common Sense Privacy and Security Measures

Monitoring

- Monitor subcontractor activities with quality assurance activities, e.g., quality check printhouse mailings
- Monitor employees for unusual activity regarding PHI/PII access




MAXIMUS 43 Helping Government Serve the People®

Common Sense Privacy and Security Measures


Shipping Packages

- Use only boxes that are intended for shipping the material you are shipping
- Make sure the box is strong enough for the weight of the material you are shipping
- Use real packaging tape to seal the box
- Consider sealing the material you are shipping in several smaller envelopes that are addressed to the intended recipient

Why should you take these steps? 

MAXIMUS 44 Helping Government Serve the People®

Common Sense Privacy and Security Measures




MAXIMUS 45 Helping Government Serve the People®

Common Sense Privacy and Security Measures


Privacy incident prevention techniques

- Conduct adequate, regular Quality Control review prior to distributing printed or electronic documents containing PHI/PII
- Ensure all workers know how to identify and report an incident
- Learn from your mistakes
- Train and educate!



MAXIMUS 46 Helping Government Serve the People®

Questions



Email the MAXIMUS Privacy Official, Ira Rothman, at IraRothman@maximus.com, or call Ira Rothman at 916.673.4152.

MAXIMUS 47 Helping Government Serve the People®
