# HIPAA Data Breach

# Objectives

- Overview of Omnibus Rule - Data Breach
- Suspected Breach - Investigation
  - Audit
  - Risk Assessment
  - Corrective Action Plan
- Written Notification Elements
- NYS Rules on Data Breach

# Objectives

- Examples of Breaches
  - Penalties

# Background ITPC

- Consulting Firm since 2004 specializing in Health Information Technology (HIT) Optimization
- 100 % Vendor  Neutral
- Hired by Organizations or Practices
  - Partnered with two legal firms as well
- Quote our Sources

# HHS/OCR

- United States  Department of Health and Human Services, Office for Civil Rights (HHS,OCR)
- HHS enforces the Federal standards that govern the privacy of protected  health information 45 C.F.R. Part 160 and Subparts A and E of Part 164, the  “Privacy Rule”
- AND the security of electronic protected health information 45 C.F.R.  Part 160 and Subparts A and C of Part 164, the “Security Rule”

# What Does a Breach Look Like?

# Breaches - HOW

- Theft accounted for 83 percent of all large HIPAA privacy and security breaches, according to Redspin, which calculated its numbers using HHS data. Some 22 percent of breaches since 2009 were due to unauthorized access, and theft or loss of encrypted devices or computers accounted for 35 percent of all breaches; hacking accounted for 6 percent.

# Begins with…

- OCR opened an investigation of Skagit County, Washington, upon receiving a breach report that money receipts with electronic protected health information (ePHI) of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County.

# And Then….

- OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules.

# Ends With

- Skagit County has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the Department of Health and Human Services (HHS) to correct deficiencies in its HIPAA compliance program.

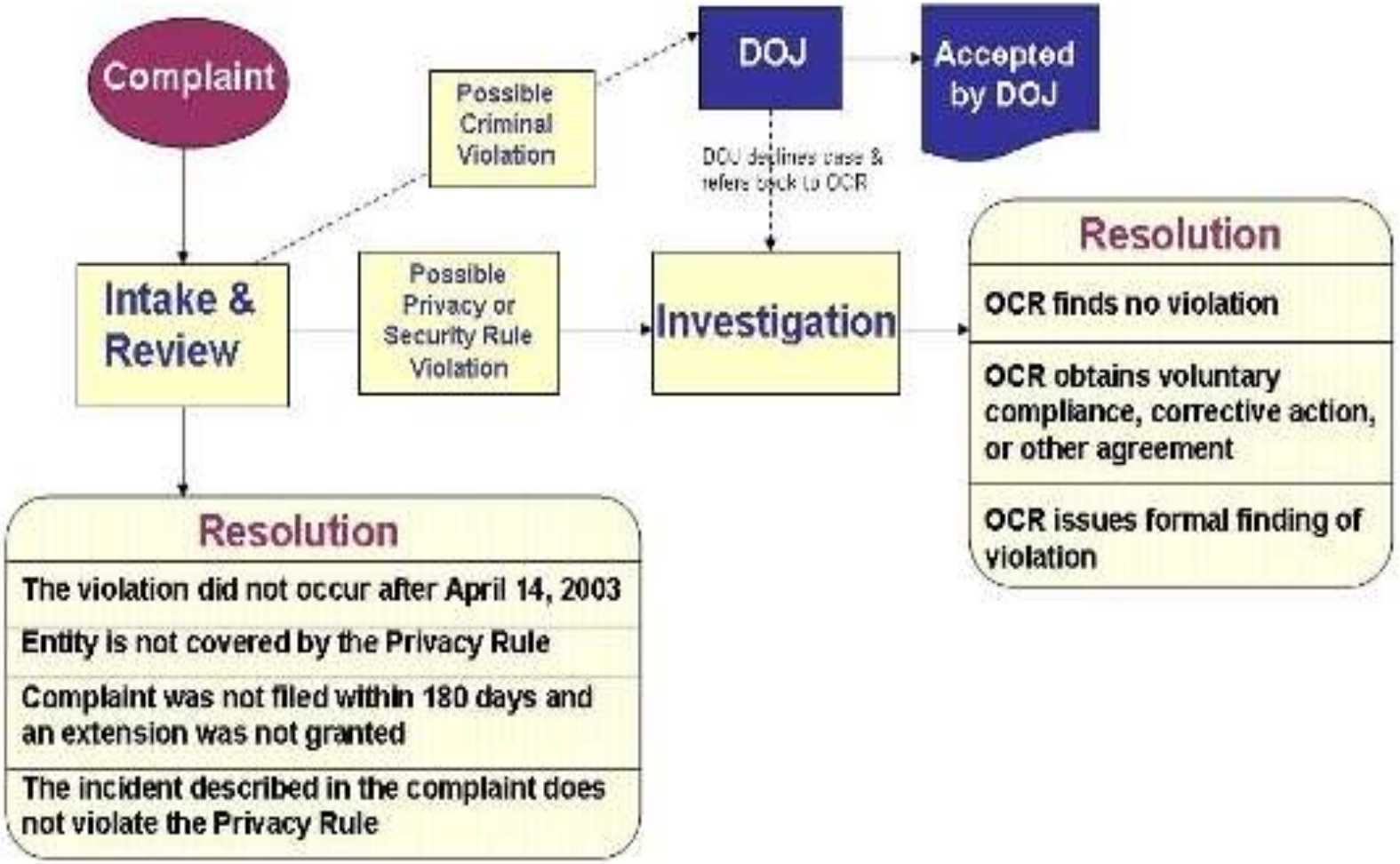
# and a Corrective Action Plan

- Skagit County shall create and revise, as necessary, written policies and procedures
- Training
  - All workforce members
  - “specific training related to the new policies and procedures”
  - certify, in writing or in electronic form, that he or she has received the required training
  - Review the training annually
  - New workforce members must have training BEFORE accessing ePHI

# Corrective Action Plan example

- Provide Substitute Breach Notification to Affected Individuals Not Previously Notified
- Hybrid Entity and Business Associate Documentation
- Security Management Process
  - Risk Assessment
  - Risk Management Measures

# HIPAA Privacy & Security Rule Complaint Process



# INTAKE

# OCR Considerations Intake and Review on ALL Complaints

- Date of complaint - must be after the rule went into affect
  - Privacy April 14, 2003
  - Security April 20, 2005
- Entity Complaint is Against
- A complaint must **allege an activity that, if proven true, would violate the Privacy or Security Rule.**
- Complaints **must be filed within 180 days** of when the person submitting the complaint knew or should have known about the alleged violation

# Covered Entities (CE)

- a health plan including but not limited to
  - health insurance companies,
  - company health plans; or
- a health care provider that electronically transmits any health information in connection with certain financial and administrative transactions (such as electronically billing insurance carriers for services): including but not limited to
  - doctors,
  - clinics,
  - hospitals,
  - psychologists,
  - chiropractors,
  - nursing homes,
  - pharmacies, and
  - dentists; or
- a health care clearinghouse.

# Business Associates Now Subject to Rules

- A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

# Entities NOT COVERED by Rules

- life insurers
- employers - (think Human Resources - employee health records)
- workers compensation carriers
- many schools and school districts,
  - many state agencies like child protective service agencies,
  - many law enforcement agencies,
  - many municipal offices

# Investigation

# Investigation

- OCR will assign an investigator/liaison
- Notify person who made the complaint
- Notify the entity in question

- Request for documents
  - EVERYTHING

# Entity Documentation - AUDIT

- What types of identifiers were exposed?
- What is the likelihood of re-identification of the information?
- Determine the probability that the protected health information could be re-identified based on the context and the ability to link information with other available information

# Entity Documentation - AUDIT

- How sensitive is the PHI, e.g., communicable disease?
- Does the unauthorized person who received the information have obligations to protect the privacy and security of the information?
- If the information impermissibly used or disclosed is not immediately identifiable, will the unauthorized person who received the protected health information have the ability to re-identify the information?

# Entity Documentation - AUDIT

- Was the protected health information ever viewed?
- Has the organization attempted to mitigate the risks to the protected health information following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances in writing that the information will not be further used or disclosed or will be destroyed ?

# Entity Documentation - Audit

- Has the organization considered the extent and efficacy of the mitigation when determining the probability that the protected health information has been compromised?
- Number of persons involved?

# OCR Resolution

- Voluntary compliance
- Corrective action - and/or
- Resolution agreement
  - May include CMP
    (Civil Money Penalty)

# Penalties

- Situations where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of a violation.
  - $100 to $50,000 per violation

# Penalties

- Violations due to reasonable cause and not to willful neglect.
  Reasonable cause .. defined: ‘‘circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.”
  - $1,000 - $50,000 PER Violation

# Penalties

- Violation was due to willful neglect that is corrected within a certain time period
  - $10,000 - $50,000 PER Violation

# Penalties

- Violation was due to willful neglect that is NOT corrected within a certain time period
  - 50,000 PER Violation

# Breach Agreement Provisions

- Between HHS, OCR and the Covered Entity
- Factual Background and Covered Conduct
- II. Terms and Conditions
  - Payment
  - Corrective Action Plan
  - Release by HHS
  - Agreement by Released Parties
  - Tolling of Statute of Limitations

# Corrective Action Plan

- Contact Persons and Submissions
  - For Covered Entity
  - For HHS
- Proof of Submissions
- Effective Date and Term of CAP
  - 120 Days
- Corrective Action Obligations
- Document Retention

# Breach Agreement Provisions

- Timely Written Requests for Extensions
- Notice of Breach and Intent to Impose CMP

# Breach Agreement Provisions

CE's Response shall have 30 days from the date of receipt of the Notice of Breach and Intent to Impose CMP, to demonstrate to HHS' satisfaction that:

1. CE is in compliance with the obligations of the CAP cited by HHS as being the basis for the breach

2. The alleged breach has been cured OR

3. The alleged breach cannot be cured within the 30-day period, but that:

(i) CE has begun to take action to cure the breach;

(ii) CE is pursuing such action with due diligence; and

(iii) CE has provided to HHS a reasonable timetable for curing the breach.

# Breach Obligations

- Varies by number of persons affected

  **Less than 500**

  – Written Notice to Individuals

  – Notice to HHS via a log and submitted annually within 60 days of the end of the calendar year

  **Greater than 500**

  – Written Notice to Individuals

  – Notice to HHS immediately

  – Notice to prominent media outlets

  – Website notification with a toll free number

# Breach Obligations NYS

- If computerized data, must notify NYS

# Contact Information

- Contact Information
  - info@itpc-corp.com
  - 585-678-1019
- Regional Offices for NYS, NJ and PR
  - 800-368-1019

# NYS Attorney General's Office

- New York State Attorney General's Office
  SECURITY BREACH NOTIFICATION
  Consumer Frauds & Protection Bureau
  120 Broadway - 3rd Floor
  New York, NY 10271
  Fax: 212-416-6003
  Email: breach.security@ag.ny.gov
-

# NYS Police

- New York State Division of State Police
  SECURITY BREACH NOTIFICATION
  New York State Intelligence Center
  630 Columbia Street Ext
  Latham, NY 12110
  Fax: 518-786-9398
  Email: risk@nysic.ny.gov

# NYS Consumer Protection

- New York State Department of State Division of Consumer Protection
  Attention: Director of the Division of Consumer Protection
  SECURITY BREACH NOTIFICATION
  99 Washington Avenue, Suite 650
  Albany, New York 12231
  Fax: (518) 473-9055
  Email:
  security_breach_notification@dos.ny.gov

# Questions

# Acronyms

- CAP - Corrective Action Plan
- CMP - Civil Money Penalty

# References

- PDF Example on the Web of Corrective Action Plan
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity_agreement.pdf
- Enforcement Process
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html