Incident Response: Are You Ready?

Chris Apgar, CISSP

Overview

- Security Incident vs. Breach
- Security Incident Planning and Your Team
- Final Breach Notification Rule – a refresher
- What Needs to be Done if a Breach Happens?
Security Incident vs. Breach

- Most security incidents are not breaches
- Security incidents include:
  - Unsuccessful attempts to hack your firewall
  - A lost encrypted laptop
  - Audit log anomalies
  - Stealing meds from a locked med cabinet
- A breach is a security incident where PHI is compromised

The Meaning of Compromised

- NIST defines “compromised” as “Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred” (SP 800-32)
Why You Need an IRP?

- A security incident response plan (IRP) HIPAA Security Rule requirement for covered entities and business associates since 2005
- Breach Notification Final Rule requires investigation, incident risk assessment and assigns burden of proof since 2009
- It’s sound security practice HIPAA or no HIPAA

Why You Need an IRP?

- Managing your risk
- Addressing vulnerabilities when they arise before they can be exploited
- OCR investigations and audits
- State Attorney Generals’ Office investigations
- Civil suit risks
Why You Need an IRP?

- Patient safety and quality of care
- Protection of clinic or hospital reputation
- Avoiding loss/churn of patients
- Prevent breaches before they happen and limit harm

Steps to Develop a Working IRP

- Senior management sponsorship
- Defining cross organizational goals
- Defining scope of IRP
- Resource commitments (cross-functional)
- Plan ownership and team leadership
- Roles and responsibilities (e.g., board, management, workforce, etc.)
Steps to Develop a Working IRP

- Preparation
  - Plan development & periodic test schedule
  - Response team education (annual & ongoing)
  - Keeping an eye on trends and risks
  - Plan review & revision (at least annually)
Steps to Develop a Working IRP

- **Identification**
  - Incident reporting: Who do I tell?
  - Incident categorization (e.g., IT infrastructure, natural disaster, theft, loss of mobile devices, etc.)
  - Risk categorization
  - Escalation requirements
  - Documentation requirements (may not require escalation – incidents often not breaches)

Steps to Develop a Working IRP

- **Identification** – if breach of PHI/PII, determine:
  - Scope of breach
  - Type of PHI/PII breached (e.g., name, Social Security number, etc.)
  - If PHI/PII was unsecure
  - Risk to individuals (four-factor risk assessment)
**Steps to Develop a Working IRP**

- Containment/Mitigation – if a breach occurs, first determine risk then initiate notification process:
  - Notify individuals
  - Notify affected health care professionals
  - Notify OCR
  - Notify media, if required

**Steps to Develop a Working IRP**

- Containment/Mitigation
  - Investigation to containment
  - Eliminate discovered vulnerability
  - Limit damage/shut down affected applications
  - Initiate disaster recovery and business continuity plan steps
  - Notify law enforcement, if applicable
Steps to Develop a Working IRP

- **Eradication**
  - Isolate affected hardware, software and data
  - Determine scope of impact following isolation
  - Initiate legal/personnel action
  - Enlist workforce members and third parties to assess physical/technical environment for potential additional damage

Steps to Develop a Working IRP

- **Recovery**
  - Restore hardware, software and data
  - Determine when to return to normal operations
  - If data corruption, restore to previous backup or flag in EHR
  - Initiate disaster recovery plan/business continuity plan
Steps to Develop a Working IRP

- Follow-up
  - Workforce training
  - Debrief and planning
  - Review of low level incidents periodically
  - Implement enhanced or new security controls
  - Audit business associates
  - Review and amend IRP as necessary
  - Review and amend DRP/BCP as necessary

Why Test Your IRP?

- Incomplete planning may result in significant harm to your organization
- Untested plans may not work as intended
- Preventable breaches occur
- Risks change and cyber crime is on the increase
- Ultimately you lose and your patients lose
Why Test Your IRP?

- Plans rely on key individuals
- If not documented and key individuals not available, successful planning may fail when ultimately tested
- Damage not relegated to just breaches of unsecure data

Testing of Your IRP

- Identify players – IT, business, clinical, vendors, etc.
- Develop incident scenario
- Schedule IRP table top test and include all team members
- Identify moderator and scribe
Testing of Your IRP

- Moderator to guide team through triage phase
- Apply IRP tools and resources (internal & external)
- Debrief and plan next steps
- Evaluate moderator and scribe notes

Testing of Your IRP

- Develop recommendations
- Revise IRP
- Modify team membership
- Train team members
- Follow up test
Testing of Your IRP

- Document your incident response plan (IRP)
- Designate a Team
- Establish your internal and external resources and tools for your IRP
- Test your IRP and annually review & revise as needed
- Review IPR following any incident

Breach Notification Rule – A Refresher

- Removed “harm” threshold and limited data set exception without ZIP code or dates of birth
- Covered entities need to report any breach unless low probability PHI has been “compromised” or used in a way that could damage individuals following required risk assessment
Breach Notification Rule – A Refresher

- Burden of proof on covered entity to show “low probability of compromise” (assumption is that notification is required)
- Effective March 26, 2013 and compliance required by September 23, 2013

Is The Breach Reportable?

- A potentially reportable breach is breach of unsecure PHI that has been compromised
- The US Department of Health and Human Services (HHS) defined secure as:
  - If electronic – encrypted according to National Institute of Standards and Technology (NIST) standards or has been completely destroyed
  - If non-electronic – shredded or destroyed
Is The Breach Reportable?

- Four-factor assessment:
  - Nature and extent of PHI involved
  - Distinguished by identifiability of data, NOT by sensitivity of data itself (e.g., HIV status vs. blood pressure readings)
  - Unauthorized person who used PHI or to whom the PHI was disclosed
  - Whether the PHI actually was acquired or viewed
  - Effectiveness of risk mitigation associated with the breach of PHI

Covered Entity vs. Business Associate

- Covered entities required to assess risk to determine if the breach is reportable
- Covered entities responsible for individual and OCR notification
Covered Entity vs. Business Associate

- Business associates and business associate subcontractors responsible for reporting breaches to covered entities
- Covered entity and business associate notification requirements did not change with the Omnibus Rule

Don’t Forget State Law

- Washington, Oregon and Alaska have enacted breach notification laws
- In Washington and Oregon a breach of unencrypted electronic PII is reportable “as soon as feasible”
- In Alaska a breach of unencrypted electronic PII or non-electronic PII represents a breach, also reportable “as soon as feasible”
Don’t Forget State Law

- In all three states "personal information" means an individual’s first name or first initial and last name and:
  - Social security number;
  - Driver's license number or Washington identification card number; or
  - Financial information
  - Passport number (Oregon only)

Don’t Forget State Law

- In Alaska a harm determination is made to determine if notification is required
- In Oregon and Washington substitute notice may be given under certain circumstances
- All three states permit delayed notification if requested by law enforcement
What Else?

- Implement:
  - Incident response policy and procedure
  - Breach notification policy and procedure
- Review, test and train – it’s an on-going process
- OCR does investigate, especially if it’s a breach of 500 individuals or more
- Don’t forget state breach notification laws

Tools & Resources for IRP

- OCR Breach Notification:
- HHS Privacy Incident Response Policy/Plan:
  [http://www.hhs.gov/ocio/policy/hhs-ocio-2010-0001.001c.html](http://www.hhs.gov/ocio/policy/hhs-ocio-2010-0001.001c.html)
- SANS “The Incident Handlers Handbook”:
Tools & Resources for IRP

- NIST IRP Planning Guide:

- NIST IRP Test Guide:
  http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

- University of California Privacy & Data Security IRP:

Tools & Resources for IRP

- Medical Practice Insider IRP Development:
  http://www.medicalpracticeinsider.com/best-practices/compliance/technology/business/patient-care/professional-development/how-develop-and

- Apgar & Associates, LLC:
  http://www.apgarandassoc.com
Q&A

Chris Apgar, CISSP
CEO & President
capgar@apgarandassoc.com