www.bipc.com

IS YOUR BUILDING SECURE FROM CYBERCRIME?
Cybersecurity and HIPAA

Brian N. Rath, Esq.

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

1

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

The Potential Breach

89% of health care organizations have suffered at least one data breach in past 2 years. – Ponemon Institute, Sixth Annual Benchmark Study on Privacy & Security of Health Care Data

- Computer lost or stolen
- USB Drive lost or stolen
- Internet-based document sharing (Google docs)
- Improper disposal of paper documents
- Theft
- Hackers/Phishing
- Ransomware

2

2

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

The Potential Breach

Additional Possible HIPAA Breaches

- Overheard staff conversations
- Overfriendly staff conversations
- Unauthorized employee access
- Emails / Reply-alls
- Social Media Use

3

3

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

The Potential Breach

Stolen Devices

Data of 43,000 patients breached after theft of unencrypted laptop

A laptop of a Coplin Health Systems employee was stolen from a car in November and serves as a reminder to healthcare organizations to encrypt all data that physically leave the building.

By Jessica Davis (/author/jessica-davis) | January 12, 2018 |

LATEST HEALTH DATA BREACHES NEWS

Michigan Medicine Admits to Healthcare Data Breach in Laptop Theft

Recent data breaches include the theft of an unencrypted laptop with PHI from an employee's car, sending snail mail to the wrong patients, and a phishing attack in Florida.

December 28, 2018 03:54 PM

Blue Cross alerts 15,000 Medicare customers of potential data breach

CHAD LIVENGOOD

TWEET SHARE SHARE EMAIL

- A subsidiary of Blue Cross Blue Shield of Michigan reported a data breach to 15,000 Medicare Advantage customers
- Laptop computer stolen in late October contained personal information
- Social Security and financial information was not contained in the stolen computer

4

4

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

The Potential Breach

Ransomware

Privacy & Security

Methodist Hospital recovering from five day ransomware attack, claims it did not pay up

Cybercriminals locked down enough of the Kentucky hospital's data that it was forced to declare an internal state of emergency. Now officials are saying they resolved the situation without giving into attackers' demands.

By **Bernie Monegain** | March 22, 2016 | 09:47 AM

5

5

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

The Potential Breach

Phishing

6

6

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy/Security Myths

- **Myth #1** – The government is only after the big guys and the huge breaches.
- **Myth #2** – We don't have an EMR system, so we don't need to worry about ePHI security.
- **Myth #3** – Business Associate Agreements are just forms we need to get signed and have in our files to satisfy the government.

7

7

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy/Security Reality

- Size doesn't matter.
- Loss or theft of laptop = likely OCR investigation.
- Failure to perform risk analysis + failure to implement policies and procedures + breach = likely big penalty.
- Encryption is a critical factor.
- Increased penalties under HIPAA Breach Notification Rule have substantially increased your risks.

8

8

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy, A Brief Overview

HIPAA Privacy/Security Rule

- Covers protected health information (PHI) in any form.
- Applies to covered entities (health care providers, health plans and health care clearinghouses) and business associates.
- Establishes patient rights.
- Defines civil and criminal liabilities.

9

9

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy, A Brief Overview

- PHI is individually identifiable health information that is:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
- PHI includes information that relates to all of the following:
  - Past, present, or future physical or mental health or condition;
  - Provision of health care
  - Past, present, or future payment for the provision of health care.

10

10

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy, A Brief Overview

HIPAA Privacy/Security Rule

- Requires Covered Entities and Business Associates to have safeguards in place to ensure the privacy of PHI.
- Denotes under what circumstances PHI may be used or disclosed.
- Gives individuals the right to examine, request a copy and make corrections to their PHI.

11

11

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy/Security Breach

- An impermissible use, acquisition or disclosure that compromises the security or privacy of the protected health information.
- Original Breach Notification Rule, a breach was defined to "compromise security or privacy" only if it posed a "significant risk of financial, reputational, or other harm" to the individual.

12

12

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy/Security Breach

- **BREACH NOTIFICATION RULE**:

An impermissible use or disclosure of PHI is ***presumed to be a breach*** and ***notification is required*** unless it is shown that there is a **low probability that the PHI was compromised**.

  - "Low probability" must be **demonstrated and documented** with a risk assessment.
  - Burden of proof of "low probability" lies with the Provider and/or BA, as appropriate.

13

13

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy/Security Breach

Exceptions to "Breach"

- Unintentional acquisition, access or use of PHI by a workforce member in the scope of duties – no further access or disclosure
- Inadvertent disclosure from one authorized person to another within a Provider/BA – no further access or disclosure
- Disclosure of PHI where Provider/BA has good faith belief that the recipient cannot retain the information

14

14

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

HIPAA Privacy/Security Breach

- Encryption Safe Harbor
- Is the PHI "secured" in accordance with the National Institute of Standards and Technology standard for encryption or destruction (PHI rendered "unusable, unreadable, or indecipherable")?
  - If yes, the Safe Harbor applies and notification is not required
  - If no, Risk Assessment should be conducted to determine the probability of compromise to the PHI

15

15

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

Breach Examples

- Computer lost or stolen
- USB Drive lost or stolen
- Internet-based document sharing (Google docs)
- Improper disposal of paper documents
- Theft
- Hackers/Phishing
- Ransomware
- Overheard staff conversations
- Overfriendly staff conversations
- Unauthorized employee access
- Emails / Reply-alls
- Social Media Use

16

16

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Phishing Emails

- **156 million** phishing email messages are sent out each day
  - **16 million** get past spam and phishing filtering tools
- In a recent survey of 2,000 people, testing phishing emails:
  - From a co-worker to schedule a meeting: 68.3%
  - From a social media site: 60.8%
  - From Dropbox, to share a file: 37.6%
  - For a software update: 26.7%
  - For social media login details: 23.9%
  - From banks: 16.6%
  - From the IRS regarding a refund: 14.7%

17

17

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

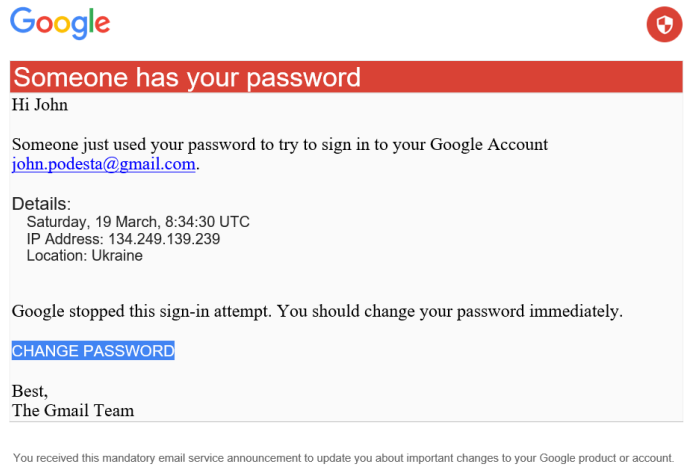
Phishing Emails

18

18

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Phishing Emails



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

19

19

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Ransomware

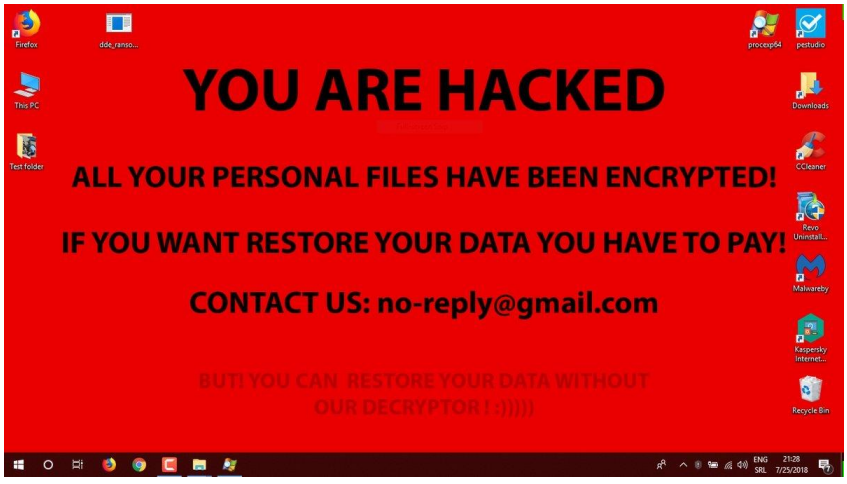
- Malicious software
- Encrypts data and renders the data unreadable and unusable.
- Once complete, user is notified that the encryption has occurred, and a ransom is demanded.

20

20

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Ransomware



21

21

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Ransomware

- Paying a ransom is not a guarantee that your data will be returned – or that it wasn't and/or won't be disclosed or the integrity compromised.

22

22

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Preparing for Potential (Inevitable?) Breach

- Ensure Security Risk Analysis and security risk management plan is thorough and up-to-date
- Create a breach response team and outside support necessary for response
- Implement clear policies on breach reporting and response, and train employees
- Be proactive with business associates
- Get good cyber-liability insurance in place

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Security Risk Analysis

- Perform a complete Security Risk Analysis (SRA) and implement a security risk management plan/policy that address all vulnerabilities identified
- Policy should trigger a re-do of the SRA if the security environment changes
- Policy should trigger a post-breach SRA if a breach is detected

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Response Team

- Identify breach response team of high-level personnel to preserve attorney-client privilege and to command attention/action
  - Administrator/management, legal, compliance, IT, communications and human resources
- Implement clear policies on breach reporting and response, and train all employees on the need for immediate reporting

25

25

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Business Associate Agreements

- Ensure that business associate agreement has aggressive time lines for reporting in the event business associate would be treated as “agent”
- Consider requiring specific security requirements
- Consider requiring cyber liability insurance
- Address responsibility for business associated-caused breaches
- Ensure BA knows who to contact at the Provider if a breach or potential breach occurs

26

26

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

- Take systems offline
- Bring in outside consultants (lawyers, forensic analysts)
  - Preserve attorney-client privilege
- Notify law enforcement
- Evaluate scope of incident
- Risk Assessment
- Data review
- Discipline or sanction of personnel that caused the breach
- Training all relevant personnel on systemic fixes that address the breach
- Documentation of all corrective actions -- retain such documentation for at least six years

27

27

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Security Risk Assessment

A risk assessment must include ***at least*** the following factors:

- Nature and extent of the PHI involved, including types of identifiers and chance 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
- The extent to which the risk to the PHI has been mitigated.

28

28

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Security Risk Assessment

- Four factors allow for fact-specific review of risk of compromise to the PHI.
- If result does not demonstrate low probability of compromise, incident must be treated as a breach.
  - Reminder: OCR considers ransomware to be a "presumed breach," so any finding of low probability of compromise must be well-supported in written RA with supporting documentation.

29

29

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Security Risk Assessment

- Risk assessments shall be "thorough, completed in good faith and for the conclusions reached to be reasonable"
- Notifications may be provided without performing the risk assessment

30

30

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Notice of Breach

- Must notify ***both*** the U.S. Department of Health & Human Services (HHS) + the affected individual of the loss, theft, or other impermissible use or disclosure of PHI
- Breaches that affect 500 or more individuals must be promptly reported to the media and HHS
  - Breaches that affect 500 or more are publicly reported on the HHS/Office of Civil Rights (OCR) website
- OCR has discretion to investigate even where there's no willful neglect

31

31

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Notice of Breach

- Individual Notice
  - In written form by first-class mail, or email if individual has agreed to receive communications electronically
  - Within 60 days of the discovery of the breach
  - If the insufficient or out-of-date contact information for 10 or more individuals, must provide substitute notice by either posting on home page for at least 90 days or notice in major print or broadcast media where the affected individuals likely reside.
  - Include a brief description of: (1) the breach; (2) the types of information involved in the breach; (3) the steps affected individuals should take to protect themselves from potential harm; (4) what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and (5) contact information

32

32

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Notice of Breach

- Media Notice
  - If breach affects more than 500 residents of a State or Jurisdiction
  - No later than 60 days
  - Press release to media in where the affected individuals likely reside
- Notice to the Secretary
  - Via the HHS web site
  - No later than 60 days if breach affects more than 500 individuals
  - If less than 500, may notify on an annual basis

33

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Post-Breach Response

Notice of Breach

- State Notice
  - New Jersey Identification Theft Prevention Act
  - Notice of unauthorized disclosure of “personal information”
  - “Personal information” is defined to include first name/initial with last name and:
    - social security number, driver’s license number or account or credit card information

34

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Penalties

4 Tiers

1. Didn't know of a violation, and wouldn't have known by exercising due diligence = **$100 - $50,000 per violation**
2. Knew, or with "reasonable diligence" would have known an act or omission violated requirement, *but* did *not* act with "willful negligence" = **$1,000 - $50,000 per violation**
3. "Conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated," *but* it was corrected = **$10,000 - $50,000 per violation**
4. "Conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated," *and* it was *not* corrected = **$50,000 per violation**

35

35

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Penalties

Factors in Penalty Amount

- Penalty amounts determined on case-by-case basis and may consider factors such as:
  - Number and extent of violations
  - Prior compliance
  - Number of individuals affected, and time period involved.
  - Nature and extent of harm
    - physical or financial harm
    - harm to reputation
    - hindered individual's ability to obtain healthcare.
- Violation of Identical Provision in Same Year – up to $1.5 million

36

36

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

Penalties

Criminal Penalties

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

Penalties

- **Settlement Amounts**
  - $16 million – Anthem, Inc. (National 2018). Phishing email opened by employee(s).
  - $3 million – Cottage Health (CA 2018). Vendor error and failure to have adequate safeguards and conducts proper risk analysis
  - $5.5 million – Memorial Healthcare System (FL 2017). Former employee log-in.
  - $387,200 – St. Luke's-Roosevelt Hospital (NY 2017). One Individual/HIV.
  - $218,400 – Catholic Health Care Services of the Archdiocese of Philadelphia (PA 2016). Business Associate breach.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Penalties

- **Criminal Conviction**
  - Two 1 year sentences – Financial worker at Alaska hospital accessed records of two kidnapping victims of drug kingpin friend and reporting status back to kingpin. (2015)
  - 18 Months in Federal prison – East Texas hospital employee accessed HIPAA PHI with intent to sell for personal gain. (2014)
  - 4 months and $2,000 fine – Former researcher at UCLA School of Medicine accessed PHI of supervisors, co-workers and celebrities after dismissal. (2010)

39

39

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

Best Practices

- A well-crafted, well-practiced security incident plan
- Be sure software is up to date and install all patches
- Make frequent backups of the system, and store backups offline
- **ENCRYPTION!!!**
- Employee Training
- Manage employee access to the system – ensure each user can only access what is necessary
- Actively manage user credentials
- Vendor management

40

40

Buchanan Ingersoll & Rooney PC | KNOW GREATER PARTNERSHIP

OPEN DISCUSSION

Brian Rath
Buchanan Ingersoll & Rooney
brian.rath@bipc.com
609-987-6827

41