BREACH BAROMETER SPECIAL REPORT

# Third-Party Breaches in 2016 Pose Alarming Risk to Patient Data

–DataBreaches.net in Collaboration with Protenus, Inc.

*At least 30% of breaches and 35% of breached records reported to HHS's public breach tool are attributable to third-party breaches.*

# Introduction

Several studies have reported that breaches involving Business Associates account for anywhere between 10% and 40% of all HIPAA breaches, with more recent statistics putting the percentage at around 30%. Enforcement actions by HHS in 2016 such as the ones below highlight efforts to get both covered entities and business associates to address the risks:

- **Oregon Health & Science University** agreed to a $2.7 million settlement in a case that addressed a number of breaches. As part of the investigation, OCR had found that OHSU stored over 3,000 individuals' ePHI in Google Drive and Google Mail without any business associate agreement in place with Google.

- **Catholic Health Care Services**, a business associate, paid $650,000 as part of settling charges stemming from the theft of an employee's cell phone that contained unprotected PHI for 412 patients.

- **Raleigh Orthopaedic Clinic** paid $750,000 as part of settling charges over their failure to have a Business Associate Agreement (BAA) in place with a firm that promised to transfer x-ray images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh turned over more than 17,000 records to the unnamed firm, who failed to return the materials.

- **North Memorial Hospital** agreed to pay $1.55 million as part of settling charges stemming from an Accretive Health incident in 2011; no BAA was in place or organization-wide risk analysis had been conducted in 2011 when a laptop with unencrypted PHI on 9,497 patients was stolen from an employee's car.

- **Advocate Health Care Network** (Advocate) agreed to pay $5.55 million to settle charges stemming from multiple breaches, one of which involved a hacking incident at its business associate, Blackhawk Consulting Group. Advocate did not have a satisfactory BAA in place with Blackhawk at the time.

# Third-Party Breaches Remain at Problematic Rates

To assess the rate and impact of third-party breaches in 2016, DataBreaches.net compiled a month-by-month recap of breaches involving business associates or vendors that were either reported to HHS or that appeared in the media or online sources from January 1 to August 31. The chronology, found at the end of this report, contains more than 60 incidents, but is undoubtedly only the tip of a much larger iceberg.

## Business Associate Breaches are More Frequent Than HHS's Breach Tool Suggests

For all entries on HHS's public breach tool going back to its inception, 17% of the entries are coded as "Business Associate" in the field "Covered Entity Type." But if one reads HHS's closing notes for incidents (more easily viewable in Excel or .csv format), it becomes clear that business associates or vendors have been involved in more incidents than statistics based on the public-facing tool might suggest.

From January 1, 2016 - August 31, 2016, only 14 out of 193 incidents (7%) on HHS's breach tool were coded "Business Associate" for "Covered Entity Type." But when DataBreaches.net recoded the breach tool entries to incorporate information available from other sources about the incidents, 57 out of the 193 incidents (30%) involved a business associate or vendor. Even that figure is almost certainly an underestimate because there were a number of incidents for which no details were available that would permit determination of whether a third party had been involved.

From discussions with some entities, it appears that when covered entities report incidents, they often do not recognize that there is a way to indicate that a business associate had been responsible for the breach. There is an option labeled, "Are you a Covered Entity filing on behalf of a Business Associate?" but some entities think, "I'm not filing on their behalf," so they don't pick that option.

**RECOMMENDATION:**
Tweak the breach tool so that the third option reads, "Are you a Covered Entity reporting a breach involving your Business Associate?"

If HHS/OCR wants entities to take business associate security seriously, it would help if the public breach tool yielded a more accurate estimate of what percent of breaches and records were were a result of business associates or third parties.

## Third-Party Breaches Have Affected Millions of Patients in 2016

For third-party incidents for which we have descriptions, the number of insider and external threats were almost identical. Insider incidents were predominantly insider errors that resulted in data exposure, or mis-mailings[1]. External incidents included hacks, theft, malware and ransomware incidents. Three incidents involved lost or missing devices or paper records.

Although insider and external incidents appeared equal in terms of frequency, that doesn't tell the whole story in terms of impact or risk of harm. Hacking incidents involving Bizmatics, Newkirk, and Quest Records affected multiple entities, and each of those incidents affected hundreds of thousands, if not millions, of individuals.

[1] Two reports involving Patterson Dental are somewhat contentious as to whether they were insider error (exposure) or hacks by an external individual(s); those reports were not included in categorizing breaches vs. insider vs. external.

## 35% of Breached Records Are a Result of Third-Party Breaches

Breaches involving business associates or vendors accounted for a somewhat disproportionate amount of affected patients and breached records for the first eight months of 2016.

HHS's figures for all 193 incidents during the relevant time period yielded a total of **12,801,481** patients affected. Based on our analysis after re-coding incidents, there were at least **4,503,464** patients affected by a breach at a third party, for a mean of **79,008** patients or records per incident. The mean number of records per incident for the 135 incidents that did not involve third parties was **62,004**. It appears, then, that breaches originating with third parties were associated with 27% more affected patients per incident than breaches originating at providers or health plans.

Based on the data used in our analyses, third-party breaches accounted for at least 30% of breaches on HHS's public breach tool and approximately 35% of patient data records breached.

## Reducing Risk

The risks of harm to patients from stolen or compromised protected health information are well-known, and growing exponentially. A recent alert from US-CERT, while not specific to health data, offers a number of useful recommendations to better protect data. Covered entities should consider whether their potential business associate or vendor adheres to these recommendations:

- *Segment networks and segregate networks based on functions*. Although firewalls are a basic staple of defense, assume attackers will get inside the perimeter, and segment the network so that even if they can access some part of the network, they cannot easily access the systems storing PHI.

- *Harden network devices*. Disable Remote Desktop Protocol and unnecessary services. If devices are connected to the network, have they been updated and patched?

- *Implement robust password policies and use the strongest password encryption available*. As hackers have repeatedly shared with DataBreaches.net in discussions of their attacks, most entities continue to use weak passwords.

As concerningly, the passwords are often left on the desktop, unencrypted. Ensuring the business associate implements and enforces strong password policies is important in protecting patient data.

- *Secure Access to Infrastructure Devices*: implement multi-factor authentication, manage privileged access, and manage administrative credentials. As US-CERT explains:

  *"Administrative privileges on infrastructure devices allow access to resources that are normally unavailable to most users and permit the execution of actions that would otherwise be restricted. When administrator privileges are improperly authorized, granted widely, and/or not closely audited, intruders can exploit them. These compromised privileges can enable adversaries to traverse a network, expanding access and potentially allowing full control of the infrastructure backbone. Unauthorized infrastructure access can be mitigated by properly implementing secure access policies and procedures."*

The alert has additional helpful recommendations, and it is important to apply these to third party providers as well. Based on reported breaches this year, we would also emphasize:

- Require encryption.

- Ensure vendors and business associates have adequate logging in place to not only log intrusion attempts but to also log what data are leaving the system. Many notifications have had to be made this year because a third party could not determine: (a) whether data had been accessed at all and/or (b) whether it had been exfiltrated.

- Include a contractual provision that termination of the contract requires the third party to securely delete all patient data - including any data that may reside in emails or backups - and to provide an attestation of secure destruction.

- Require vendors or business associates to provide adequate training to their employees so that they are less likely to fall for social engineering or phishing attacks.

- Ensure that third-party providers have anti-virus and malware protection and that it is kept updated.

- Require the third-party provider to maintain regular backups so that in the event of a successful ransomware attack, the system can be restored from backup with minimal data loss;

- Update and patch all software promptly and include a contractual obligation for the vendor or business associate to do the same.

With OCR cracking down, and with the Federal Trade Commission flexing its muscle in the healthcare sector, this is a good time for covered entities and their providers to update risk assessments and to implement more technical safeguards for protected health information. But increasing technical safeguards is only one aspect of improving data protection.

Robert Lord, CEO and co-founder of Protenus, stresses that "improving protection of patient data in the EHR is not a single project or checklist. It should be an on-going, living process that strives for continuous improvement. " He recommends the following five tips to reduce Business Associate risk:

1. Ensure you have up-to-date Business Associate Agreements (BAA) in place with every vendor. Have a process to both standardize and regularly review this process, as these documents form the legal core of your BA management program.

2. Retain and update Human Resources (HR) data to understand individual users and their roles within your system. Managing the identities of everyone who has access to your EHR is critical, whether an employee or a BA.

3. Implement a proactive security posture as opposed to a reactive one. Deploy a privacy analytics platform that can identify and resolve privacy violations quickly and efficiently to save your organization major costs associated with a public breach.

4. Conduct regular, on-going risk assessments based as changes that occur within your system. Foster a cultural shift from the "once per year" interpretation of Risk Assessments to one of ongoing review that is based on the degree of organization change occurring at any given time.

5. Understand the risks associated with subcontractors to your BAs. Ask to review the sBAAs (Subcontractor Business Associate Agreements) with BAs that have access to an extensive amount of your data.

If HHS follows the recommendation made by databreaches.net, we hope the industry will get a more accurate estimate of the prevalence and scope of third-party breaches. In the interim, we encourage covered entities to require greater physical and technical safeguards for PHI held by third parties and to audit compliance with those requirements throughout the year.

**

## About DataBreaches.net

DataBreaches.net is a web site devoted to reporting on data security breaches, their impact, and legislative developments relevant to protecting consumer and patient information. In addition to providing news aggregation from global sources, the site also features original investigative reporting and commentary by the site's owner, a healthcare professional and privacy advocate who writes pseudoanonymously as "Dissent."

## About Protenus

Protenus is a proactive patient privacy analytics platform that protects patient data in the EHR for some of the nation's top-ranked hospitals. Our advanced platform for alerting, forensics and reporting replaces costly consulting services, ineffective and outdated rules engines and traditional

compliance offerings. Using data science and machine learning, Protenus technology uniquely understands the clinical behavior and context of each user that is accessing patient data to determine the appropriateness of each action, elevating only true threats to patient privacy and health data security.

# Third-Party Breaches Involving Health Information

## January 1 - August 31, 2016

### Compiled by DataBreaches.net

The chronology below includes breaches where a business associate or vendor experienced a security or privacy incident that may have compromised individuals' protected health information or health data. The list includes not only HIPAA-covered entities, but also businesses or other entities that collect or maintain health information. In some cases, all we have is a report to HHS without any details or publicly available information.

### JANUARY:

- Blue Shield of California announces that an **unnamed vendor** had notified it that 20,764 members' information may have been accessed by an unauthorized user who gained access to the vendor's data systems.

- An error by patient portal vendor **Greenway Health** exposed 1,000 Florida Medical Clinic, PA patients' balance due information to those logged in with industrial accounts.

- Virtua Medical Group learned that its **unnamed transcription vendor** made a configuration error during an upgrade that resulted in 1,654 patients' transcription records becoming viewable on the internet.

- Livongo Health learned that its **unnamed business associate** mislabeled packages containing lancet devices. The devices were delivered to the correct address, but the shipping label stated the wrong name for 1,950 of the CE's members.

### FEBRUARY:

- A researcher discovers thousands of dental patients' information exposed on a publicly available Patterson Dental FTP server. Of the exposed

records, 4,293 were from the Massachusetts General Hospital Dental Group.

- **Seim Johnson LLP** reported on behalf of 10 unnamed health care provider clients that an employee took his firm-issued laptop computer on a non-business weekend trip. When the employee arrived home from this trip, he discovered the backpack containing the laptop was missing. The laptop contained the protected health information (PHI) of 30,972 patients.

- **DataStat** reported that it had erroneously misdirected surveys to 487 individuals after failing to follow the BA's re-print protocol after a printer paper jam. The breach affected 552 patients of the unnamed covered entity.

- **BlueCross BlueShield of South Carolina** reported, as a business associate of the South Carolina Public Employee Benefit Authority, that it had incorrectly mailed pre-authorization dental letters to 998 individuals.

- Radiology Regional Center, PA, announced that it was informed by its records disposal vendor, **Lee County Solid Waste Division**, that records had fallen off the truck. They would subsequently report that 483,063 patients were potentially affected, although they believed that all flyaway records had been retrieved.

- Children's National Medical Center became aware that **Ascend Healthcare Systems**, an outside dictation vendor, had inadvertently misconfigured a file site and allowed access from the Internet to transcription documents for as many as 4,107 patients via a FTP server. Of special note: according to CNMC, the data never should have been on Ascend's FTP server in February, because CNMC terminated its contract with Ascend on June 23, 2014, and as part of the separation, "Ascend was contractually obligated to delete all Children's patient information."

- An **unnamed vendor** of Mayfield Brain & Spine was compromised and 23,341 patients were sent an email with a virus-infected attachment.

Recipients who clicked on the attachment were infected with ransomware.

- An **unnamed vendor** placed files containing 1,185 Carle Health patients' information on Carle's server in a way that potentially allowed them to become viewable to those who had access to that server via the internet.

- **EqualizeRCM Services**, a vendor providing billing and collection services to healthcare providers, had a laptop stolen from an employee. The laptop contained patient information on some patients seen at Northstar Healthcare Surgery Center (Scottsdale, Houston, Dallas), Microsurgery Institute (Houston, Dallas), Hermann Drive Surgical Hospital, Victory Medical Center Houston, Central Dallas Surgery Center, Southwest Freeway Surgery Center, Kirby Surgical Center, and Plano Surgical Hospital. The total number of patients affected was not disclosed.

### MARCH:

- Reports from clients of **Bizmatics, Inc**., provider of PrognoCIS software, begin emerging. Bizmatics was hacked as early as January, 2015, but the breach was not discovered until December, 2015. By August, 2016, we were still learning of clients who had been affected. OCR closed its investigation of Bizmatics after the firm implemented some corrective actions to prevent a recurrence. Clients reporting the incident to HHS included Eye Associates of Pinella, Lafayette Pain Care, Family Medicine of Weston, Illinois Valley Podiatry Group, Complete Chiropractic & Bodywork Therapies, Integrated Health Solutions, California Health & Longevity, ENT & Allergy Center, My Pediatrician, PA, The Vein Doctor, Vincent Vein Center, Grace Primary Care, North Ottawa Medical Group, Uncommon Care, Arkansas Spine & Pain, Lifewellness Institute, Pain Treatment Centers of America , Complete Family Foot Care, HeartCare Consultants, and Mark Anthony Quintero. There may be other entities affected by this incident that have not been publicly linked to the breach. There are multiple articles about this breach on DataBreaches.net.

- Medical documents containing names and Social Security numbers for hundreds of patients were found dumped on a sidewalk. The records belonged to Chula Vista-based Modern Home Health Care, who stated that they had an **unnamed vendor** under contract to provide shredding services.

- The personal information of 2,451 Kaiser Permanente members on the Inland Empire Health Plan was in a stolen mail delivery truck in Santa Clarita. The **delivery vendor was not named.**

- A laptop with unencrypted information on 6,229 OptumRx patients was stolen from an **unnamed vendor's** employee's car.

- An Alabama CVS reported that the password-protected laptop with information on 1,000 patients had been stolen from an **unnamed vendor** in Indianapolis. This may be the same incident affecting OptumRx patients, above.

- Metropolitan Jewish Health System, Inc. d/b/a MJHS reported a phishing incident affecting 2,483. Although they reported it to HHS as involving a business associate, they seem to be referring to participating programs and agencies.

### APRIL:

- **Target Corporation Health Plan** reported a breach to HHS that affected 719 members. **Sisters of Charity of Leavenworth Health System Health Benefits Plan** reported a breach affecting 540 patients to HHS, and **Pacific Gas and Electric Company** reported a breach to HHS that affected 2,426 individuals. No details were available, but all three reported that a business associate was involved and that their breaches involved unauthorized access/disclosure of PHI on paper/films.

- Midland Memorial Hospital discovered that a physician who previously had privileges at the hospital and was formerly employed by **Premier Physicians**, left patient information at a private residence, causing the

information to be accessible to certain members of the public. Midland Women's Clinic and Premier Physicians also reported related incidents to HHS, bringing the total number affected to 3,511.

- An error made by an **R-C Healthcare Management** employee resulted in 651,971 Bon Secours patients having their PHI exposed on the internet.

- **Quarles & Brady, LLP** reported as a business associate the theft of a laptop with information on 1,032 individuals. The covered entity or entities was/were not named on HHS's breach tool.

- A records management vendor, **Quest Records LLC**, had a security incident that appears to have resulted in the compromise of its clients' login credentials. The breach, which is still under investigation, may have contributed to a number of hacks of healthcare entities by TheDarkOverlord, including Athens Orthopedic Clinic, who reported that 201,000 patients were affected. Other hacks by TheDarkOverlord that have been linked to third parties include the Midwest Orthopedic & Spine incident and the Prosthetic & Orthotics incident.

- Comanche County Memorial Hospital disclosed that an **unnamed vendor** had made an error in e-mailing satisfaction surveys to 2,199 patients of Memorial Medical Group (MMG).

- Florida Hospital Medical Group notified HHS that an unnamed transcription service had mistakenly sent unencrypted emails with patient information to doctors; 1,906 patients were notified.

**MAY:**

- Blaine Chiropractic Center reported that they had discovered unauthorized software installed by an unknown person using a hidden administrator account that "had been created and subsequently made hidden by our **[unnamed] third party** software vendor at the point of installation of our patient record software." The center was not sure

whether patient information had been accessed, and so notified 1,945 patients.

- **Surgical Care Affiliates** reported a stolen laptop containing information on 9,009 patients. The covered entity or entities was/were not named on HHS's breach tool, but DataBreaches.net reported that it was Blue Ridge Surgery Center.

- An **unnamed vendor** that processes and mails refund checks for Walmart made a printing error that exposed 27,392 patients' information.

**JUNE:**

- Mercy Medical Center Redding learned that a business associate, **NaviHealth**, had discovered that one of their case managers was working under a stolen identity. The center notified 520 patients.

- Texas Health & Human Services Commission disclosed that its documents storage vendor, **Iron Mountain**, could not locate 15 boxes of records from three storage facilities. The incident reportedly affected 600 patients.

**JULY:**

- **Newkirk Products** is a business associate that issues healthcare ID cards for health insurance plans. A hack discovered in July reportedly affected 3,466,120 members of Blue Cross and Blue Shield of Kansas City, Blue Cross Blue Shield of North Carolina, HealthNow New York Inc., BlueCross BlueShield of Western New York, BlueShield of Northeastern New York, and Capital District Physicians' Health Plan, Inc. (CDPHP), and, through Newkirk's relationship as a service provider to DST Health Solutions, Inc., Gateway Health Plan, Highmark Health Options, West Virginia Family Health, Johns Hopkins Employer Health Programs, Inc., Priority Partners Managed Care Organization, Uniformed Services Family Health Plan, and Symphonix Health.

- **Marin Medical Practices Concepts** provides medical billing and electronic medical records services to many Marin physicians and the county health

clinics. Its computer system was hacked and they paid a ransom to regain access to their data. Doctors were reportedly unable to access locked-up patient records for at least 10 days.

- **Ambucor Health Solutions**, an unincorporated division of The ScottCare Corporation, reported a breach to HHS that affected 1,679.

- Sunbury Plaza Dental reported a burglary at an **unnamed storage vendor** affecting 7,784.

- An employee of a health care revenue company, **Cardon Outreach**, looked at nearly two dozen AnMed Health patient records without authorization.

### AUGUST:

- Harbin Clinic learned that documents storage vendor **Iron Mountain** cannot locate several boxes with 498 patients' medical records.

- Southwest Portland Dental reported a breach to the Oregon Attorney General's Office involving **Patterson Dental**. This appears to be related to a similar breach reported by a researcher in February, but these data were not in the exposed data he had uncovered, suggesting that there may have been other files or folders also exposed.

- CHI Franciscan Health Highline Medical Center ("Highline") in Washington reported that 18,399 of their patients were also affected by the **R-C Healthcare Management** incident previously reported by Bon Secours.

- The VA Medical Center in Milwaukee notified 21 veterans after the **Medical College of Wisconsin** (an "academic affiliate") notified them that an employee's email account had been compromised. The VA noted that the employee had "mismanaged" their account security. All told, 3,200 patients were notified by the college.