Breach #77

Description:

1. An employee of a business associate (BA), naviHealth, provided services to the covered entity's (CE) patients using an assumed name and nursing license from June 1, 2015, to May 13, 2016, and accessed protected health information (PHI) in the course of employment.
2. The breach affected 520 individuals who were patients of the CE's Redding facility and a total of 1,253 Dignity Health patients in California and Nevada.
3. The types of PHI involved in the breach included full names, addresses, dates of birth, social security numbers, claims information, diagnoses/conditions, lab results, and medications.
4. The CE provided breach notification to HHS, affected individuals, and the media and also provided substitute notice.
5. OCR reviewed the BA agreement in place between the CE and BA and obtained assurances that the CE implemented the corrective actions listed above.
6. In response to the breach, the BA sanctioned the responsible employee, terminated the employee's access to all PHI, and contacted law enforcement to report the incident.
7. The BA also reviewed recorded calls made by the employee and PHI accessed by the employee to ensure that PHI was accessed to provide patients with services according to the job function.
8. In addition, the BA improved administrative safeguards by revising its workforce clearance policies and procedures.

Breach #147

Description:

1. On December 30, 2015, a Valley Hope Association employee's work-issued laptop computer was stolen from her vehicle.
2. The incident affected approximately 52,076 individuals.
3. The protected health information (PHI) stored on the laptop included names, addresses, dates of birth, phone numbers, social security numbers, medical record numbers, treatment types and locations, as well as health insurance, financial, and medication information.
4. The employee immediately reported the incident to the local police and the covered entity (CE).
5. The CE conducted a forensic analysis and concluded that the system had not been accessed following the theft.
6. Following the breach, the CE terminated the computer's access to its computer network, reset the user's password, and verified the laptop had no open connections to other electronic systems.
7. The CE encrypted all devices containing PHI and implemented the use of software to mask social security numbers.
8. The CE also developed an information security and privacy committee, updated its policies and procedures manual, and trained staff on its updated policies and procedures relating to password use and development, automatic time outs on electronic devices, malicious malware, and network access rights.
9. The CE provided breach notification to HHS, affected individuals, and the media and posted substitute notice on the home page of its website.
10. OCR obtained assurances that the CE implemented the corrective actions listed above.

Breach #162

Description:

1. OCR opened an investigation of the covered entity (CE), New West Health Services, dba New West Medicare, after it reported that an employee's unencrypted laptop computer was stolen from a hotel meeting room.

2. The types of electronic protected health information (ePHI) involved in the breach included demographic information, social security numbers, Medicare claim numbers, financial information, diagnoses, medical histories, and prescription information, and affected 28,209 individuals.

3. The CE provided breach notification to HHS, affected individuals, and the media and provided individuals' with free credit monitoring and identity theft protection services.

4. Following the breach, the CE improved safeguards by recalling all of its laptops to ensure they were encrypted, installing geo-location capabilities on all of its laptops, and installing remote wiping software on all of its company-issued BlackBerry devices.

5. The CE also sanctioned the employee whose laptop was stolen, retrained its staff on HIPAA privacy and security requirements, and created a new data incident response plan.

6. OCR obtained assurances that the CE implemented the corrective actions noted above.

7. Due to financial considerations, the CE announced that it will cease all operations in 2017 after it fulfills its 2016 insurance plan requirements.

Breach #202

Description:

1. An employee of a business associate (BA), Centene Management Company, impermissibly downloaded several data files containing the protected health information (PHI) of 8,208 individuals to an unauthorized removable storage device and then resigned from the organization.
2. The former employee returned his company issued laptop on March 23, 2015.
3. However, in violation of standard procedures, the laptop was not connected to the network for processing/reimagining at the time it was returned which allowed the impermissible downloads to go undetected.
4. On October 8, 2015, a data loss prevention tool discovered the impermissible downloads when the former employee's laptop was connected to the network for processing.
5. The PHI involved in the breach included names, addresses, dates of birth, medical identification numbers, and in some cases social security numbers.
6. The PHI downloaded belonged to members of the covered entities, Bridgeway Health Solutions and Superior Health Plan.
7. The BA provided breach notification to HHS, affected individuals, and the media and also provided substitute notice.
8. In response to the breach, the BA implemented and communicated a policy to help ensure the timely processing of returned information technology equipment.
9. It also implemented a policy and software solution prohibiting the downloading of data to unauthorized, external storage.
10. OCR provided technical assistance regarding the risk analysis and risk management provisions of the Security Rule.

Breach #216

Description:

1. On May 18, 2013, OCR received an anonymous complaint alleging that the protected health information (PHI) of the patients of the covered entity (CE), Dr. Daniel Sheldon, M.D., P.A., was accessible on the internet via Google.

2. OCR confirmed the allegations when it identified web search results containing private medical records from a website associated with the practice.

3. Following an investigation by OCR, the practice submitted a breach notification to HHS on September 16, 2015, in which it reported that the PHI of approximately 2,075 patients was potentially viewable online, including addresses, dates of birth, names, and clinical information.

4. In response to the incident, the CE contacted its electronic medical record ("EMR") hosting company, IOS Health Systems ("IOS"), which immediately secured the information and conducted an internal investigation.

5. IOS changed the file locations of the practice's EMR records, renamed the file structures, obfuscated file directories, conducted standard security inspections, and began an audit trail review to determine any unauthorized access to the CE's records.

6. Additionally, the CE ensured that users did not share any documents or links via non-secure methods, changed all passwords for all users, confirmed username and password confidentiality policies with all employees, ensured proper antivirus and spyware applications were installed, and verified that its firewall was properly configured with the latest version of security upgrades.

7. In response to OCR's investigation, the practice provided evidence that provided breach notification to HHS, affected individuals and the media, and offered identity theft protection services.

8. It also terminated its relationship with its EMR system hosting company, IOS, and entered into a revised business associate agreement with a new EMR hosting company.

9. Finally, the CE created new policies regarding its breach notification procedures.

Breach #233

Description:

1. A physician's backpack containing five unencrypted portable data drives and a handwritten notebook with the protected health information (PHI) of approximately 1,004 pediatric patients was stolen from an automobile.
2. The types of PHI involved in the breach included names, dates of birth, hospital medical record numbers, types of surgery performed, and treating physicians' names.
3. One of the drives contained surgical images of twenty patients.
4. The breach affected approximately 876 patients of Texas Children's Hospital (TCH) and 128 patients of Memorial-Hermann.
5. The physician, a surgical fellow for the covered entity (CE), Baylor College of Medicine, reported the theft to the police and notified TCH.
6. TCH initiated an investigation and notified the CE of the breach on July 15, 2015.
7. The CE provided breach notification to HHS, affected individuals, and the media.
8. Following the breach, the CE distributed an acknowledgment and attestation document to each medical resident and fellow addressing the CE's patient privacy and security policies, including incident reporting procedures.
9. Due to OCR's involvement, all residents, fellows and learners are required to complete the acknowledgment and attestation at the beginning of each academic year.
10. The CE also initiated a policy to require the acknowledgment and attestation to be included in each graduate medical education program participant's contract at the beginning of each academic year.

Breach #286

Description:

1. The covered entity (CE), Clinical Reference Laboratory, Inc. sent a parcel to Massachusetts Mutual Life that was opened and damaged during the mailing process by the United States Postal Services (USPS).
2. The damaged parcel contained the protected health information (PHI) of approximately 864 individuals, including names, partial and full social security numbers, dates of birth, and clinical test codes.
3. OCR received two other breach reports from the CE which involved the same or similar fact patterns as the breach report for this case.
4. OCR consolidated these investigations into one breach compliance review.
5. The CE investigated the breaches and concluded that the likelihood of misuse or further disclosure of the PHI was remote since the USPS confirmed that all unmatched pages were segregated and shredded.
6. The CE provided breach notification to HHS, affected individuals, and notified appropriate authorities required by each jurisdiction that included an affected individual.
7. The CE also offered affected individuals a free two-year subscription to credit monitoring services and credit report controls.
8. Following the breach, the CE appointed a new privacy officer, who was required to complete HIPAA training, and verified that its workforce received HIPAA-related training.
9. The CE also implemented a new breach reporting procedure and initiated the implementation of a secure online portal for clients to obtain PHI electronically.
10. OCR obtained documentation evidencing that the CE implemented the corrective actions listed.

Breach #292

Description:

1. The covered entity (CE), Allina Health, erroneously mailed a number of letters to patients about preventative screenings which resulted in individuals receiving a letter and a screening sample collection kit at their address, but labeled with another individual's name.
2. Two business associate (BA) vendors were also involved in processing the mailing.
3. The breach affected approximately 838 individuals and the protected health information (PHI) involved in the breach included individuals' name.
4. Following the breach, the CE immediately ceased mailing preventative screening kits until it was able to complete an investigation to determine the root cause of the breach, which included reviewing its business associate's practices regarding the mailing of the screening kits to ensure it had quality control processes in place and were appropriately followed.
5. The CE also initiated and implemented its incident system to timely and effectively manage the investigation, patient notification, and risk mitigation.
6. The CE provided breach notification to HHS, affected individuals, media outlets, and a Minnesota state senator.
7. The CE engaged an outside vendor to mail the individual notifications and establish a call center to accommodate any patient inquiries.
8. The CE also implemented a new workflow in its mailing processes to reduce the number of manual steps and incorporated an additional quality check so as to reduce the potential for error and to ensure the accuracy of mailing lists.
9. The CE also retrained its employees on safeguarding PHI when mailing correspondence, and verified that its employees received the training.
10. OCR obtained documentation evidencing that the CE implemented the corrective actions listed.

Breach #419

Description:

1. An employee of the covered entity (CE), Penn State Milton S. Hershey Medical Center, downloaded protected health information (PHI) onto an unsecured flash drive and used the device in his personal computer to complete work which he then emailed to the CE using his personal email account.

2. The types of PHI involved in the breach included the demographic and clinical information for 1,801 individuals.

3. The CE provided breach notification to HHS, affected individuals, and the media.

4. Following the breach, the CE performed a risk assessment and updated encryption measures.

5. The CE also reminded all clinical laboratory staff and faculty of expected practices pertaining to safeguarding PHI, and provided staff a listing of the relevant policies concerning encryption and electronic messaging and links to the corresponding policies.

6. As a result of OCR's investigation, the CE submitted to OCR copies of its policies regarding use of personal devices and emails, storing PHI on third party owned or managed media and use of approved electronic connections, systems and/or services.

7. OCR verified that appropriate policy was in place at the time of the incident and the employee did not follow the policy.

8. OCR obtained assurances that the CE has implemented the corrective actions listed above.

Breach #441

Description:

1. The covered entity (CE), Greenwood Leflore Hospital, discovered that an ex-employee of a business associate (BA) the CE used to recycle and destroy old x-ray films, stole x-ray films which contained the names, dates of birth and x-ray images of 3,750 patients.
2. This individual's employment had been terminated by the BA prior to the breach, and therefore he was not authorized to take possession of these x-ray films.
3. The CE provided breach notification to HHS, affected individuals, and the media, and also posted substitute notice.
4. In response to the breach, the CE filed a police report, attempted to recover the x-ray films, and sanctioned and re-trained the employees involved.
5. The CE also filed a civil lawsuit against the individual who took the films.
6. The individual was later arrested and found guilty of petit larceny and was ordered to pay restitution to the CE.
7. The CE provided additional training to its entire workforce regarding its BA access and breach policies, and terminated its business relationship with the BA.
8. OCR obtained the CE's policies and procedures related to the cited Privacy Rule provisions, as well as documentation related to employee training on the Privacy and Security Rules.

Breach #470

Description:

1. On January 10, 2014, a business associate (BA), PracMan, Inc., of two covered entities (CE), Monarch Women's Health (Monarch) and Punuru J.M. Reddy, M.D., Inc. (Dr. Reddy), impermissibly disclosed the protected health information (PHI) of the CEs' patients when the BA's technology subcontractor, MASHNet, copied and stored computer files in error on an unsecured server.

2. The PHI included demographic, clinical, and financial information, including names, account numbers, insurance providers, procedures, diagnoses, social security numbers (SSN), and account balances affecting approximately 1,179 of Dr. Reddy's patients and approximately 1,145 of Monarch's patients.

3. The BA provided breach notification to HHS, affected individuals, and the media.

4. It also established a toll-free number and website dedicated to providing information regarding the breach, and offered one year of free credit monitoring to individuals whose SSN was potentially exposed online.

5. In response to the breach, the BA engaged a third party to perform a risk analysis of its operations and updated its privacy and security policies.

6. The BA ensured that the data was removed from the unsecured server and all cached copies of links to the PHI were removed.

7. OCR obtained assurances that the BA implemented the corrective actions listed above.

8. Additionally, the BA terminated its relationship with the subcontractor and restructured its corporate network.

Breach #478

Description:

1. The covered entity (CE), University of Miami Health System, reported that on or around June 27, 2013, it learned from Iron Mountain, its business associate (BA), that 15 boxes containing patients' protected health information (PHI) were lost during the transfer between its new and old storage/shredding vendors.
2. The boxes contained a mix of billing and research records of 13,074 patients that included financial and clinical information.
3. Following the breach, the CE provided breach notification to HHS, affected individuals, and the media and also posted substitute notice on its website.
4. The CE offered credit monitoring and identity theft protection to all affected individuals.
5. The CE and BA reviewed the BA's processes for the transfer, pick up, and storage of records and worked together to revise procedures for safeguarding archived PHI.
6. The CE required the BA to re-train all of its personnel who handle the CE's data and re-trained its workforce on its HIPAA Privacy and Security policies and procedures.
7. Additionally, the CE hired a new HIPAA Privacy Officer, revised procedures for retaining records in order to avoid sending records containing billing information to off-site storage, and developed a new sanctions policy specific to privacy violations.
8. The CE also improved technical safeguards by implementing the Fair Warning System, a cloud-based security solution.
9. OCR obtained assurances that the CE implemented the corrective actions listed above.

Breach #515

Description:

1. A patient scheduler at one of the covered entity's (CE) small subsidiary offices impermissibly accessed the electronic health record (EHR) system via a virtual private network (VPN) and took photographic images of patient data, which she tried to download for printing at Wal-Mart.
2. She accessed the records of about 4,400 patients and photographed those of 430.
3. The protected health information (PHI) involved in the breach included names, addresses, dates of birth, social security numbers, and telephone numbers.
4. The suspect behavior at Wal-Mart was investigated by the County Sheriff, who informed the CE of the breach.
5. The CE provided partial breach notification to affected individuals, HHS, the media, and provided substitute notice on its website.
6. Following the breach, the CE discharged the workforce member and terminated her access to the EHR. The CE updated its privacy and security plan and employee handbook.
7. In addition, the CE improved safeguards by limiting access to its VPN to providers and administrators, and instituted routine weekly audits of EHR system use.
8. After OCR began its review, the covered entity retrained the office manager and the provider who had been at the office where the breach occurred.
9. As a result of OCR's investigation the CE received technical assistance on the complete requirements for breach notifications.

Breach #526

Description:

1. An employee of the covered entity's (CE) business associate (BA), Island Peer Review Organization, lost an unencrypted and not password-protected portable computer drive (a "USB" drive) that contained 9,825 patients' names, addresses, dates of birth, social security numbers, clinical information, diagnoses, conditions, and identification numbers (including member identification, Medicaid identification, subscriber identification, patient account number and patient control number).
2. The CE, New Jersey Department of Human Services, provided breach notification to HHS, and the BA notified affected individuals and the media.
3. Following the breach, the BA recovered all of the USB drives used by employees and retrained these employees on the BA's security policies and the appropriate use of encryption on portable electronic media.
4. As a result of OCR's investigation and technical assistance, the BA retrained certain staff and implemented a policy requiring staff to use only portable media purchased by the BA's Information Systems Department.
5. The BA installed technical safeguards on all computers so only approved portable devices are allowed access while any other types can be rendered as "read only" or unusable.
6. Further, the CE indicated that the BA's device access will be monitored and logged to guard against employees who attempt to copy data to unauthorized devices.
7. OCR advised the CE of the requirements to perform a thorough and accurate risk analysis and establish a risk management plan.

Breach #533

Description:

1. On September 11, 2013, a patient of the covered entity (CE), Associated Urologists of North Carolina (AUNC), notified the CE that when he did an internet search for his name he was able to see a list identifying him as an AUNC patient.
2. The CE investigated and discovered that protected health information (PHI) was accessible on the internet from September 17, 2012, to September 11, 2013, and that the breach was due to the way medical notes had been transcribed.
3. An employee uploaded audio files and lists of patients' names through a file transfer protocol (FTP) site to assist with transcription.
4. The files included the names, dates of birth, phone numbers, referring physicians, chart numbers, and reasons for visits for 7,297 patients.
5. In response to the incident, the CE immediately discontinued use of the FTP site, removed all of its files from the unsecure website, and contacted Google to have all cached copies of the files removed.
6. The CE also provided breach notification to HHS, affected individuals, and the media and offered free credit monitoring and a toll free number to answer questions.
7. The CE also reviewed its policies and retrained all staff on it data privacy and information security policies.
8. Additionally, the CE partnered with a security contractor to develop and implement new policies and procedures to safeguard electronic PHI.
9. OCR obtained assurances that the CE implemented the corrective actions listed above.

Breach #556

Description:

1. A newly hired janitorial service mistakenly disposed of information face sheets awaiting removal from the covered entity's (CE) Breach Center to shredding bins before the face sheets could be shredded.

2. The face sheets belonged to the CE, Rose Medical Center, a Hospital Corporation of America facility, and contained protected health information (PHI), including demographic information, social security numbers, insurance information, physician information and next of kin contact information for approximately 606 individuals.

3. The CE provided timely written notice to affected individuals, HHS, and the media.

4. As a result of OCR's investigation, the CE instituted a new procedure whereby all documents containing PHI must be disposed of directly into secured shredding bins, rather than recycling bins.

5. The CE also launched a company-wide initiative to implement improved procedures to safeguard social security numbers, such as removing the numbers from documents where possible, and minimizing the printing of documents containing such PHI.

6. The CE also retrained staff on the HIPAA Privacy Rule.

7. Finally, the CE's Breast Center ceased printing duplicate face sheets and full social security numbers on face sheets.

Breach #570

Description:

1. A workforce member of the covered entity (CE), Sierra View Medical Center, impermissibly accessed an internal hospital roster covering different departments over a period of several days between July and August 2013, which potentially affected the electronic protected health information (ePHI) of approximately one thousand nine (1,009) individuals.
2. The ePHI included patients' names, room numbers, treating physicians' information, diagnoses, and medical record data, including treatment notes.
3. The CE provided breach notification to HHS, affected individuals, and the media.
4. The CE investigated and determined that the employee had not used the information, despite impermissibly accessing it.
5. The CE sanctioned the employee, implemented compliance actions to meet workforce security standards, including log-in monitoring.
6. The CE also revised policies and procedures and conducted training on the security awareness standard.
7. OCR provided substantive technical assistance and identified corrective actions that the CE must complete to comply with the Security Rule, which includes the following:
   (a) conduct and monitor a comprehensive, enterprise-wide risk analysis,
   (b) update and monitor its risk management plan, and
   (c) monitor its information access management to ensure adequate safeguards of ePHI.

Breach #597

Description:

1. The covered entity (CE), Sheet Metal Local 36 Welfare Fund, reported that an employee of its business associate (BA), People Resources Corporation, inadvertently uploaded Excel spreadsheets containing the CE's Member Assistance Program (MAP) eligibility data onto an unsecure website maintained by the BA.
2. An unknown individual or entity believed to be in China uploaded the data to two additional websites.
3. In addition, two other websites contained links to the BA's unsecure website.
4. The spreadsheets contained the names, addresses, dates of birth, and social security numbers of 4,560 members (but not dependents).
5. The BA was purchased by E4 Health, Inc. in September 2013.
6. The CE provided breach notification to HHS, affected individuals, and the media.
7. The BA immediately removed the protected health information (PHI) from the unsecure website, confirmed that the PHI was no longer available on its websites or through internet search engines, and confirmed that only one spreadsheet was accessed by unauthorized parties and the other spreadsheets had not been viewed or compromised.
8. The BA adopted additional protections to prevent future unauthorized disclosures (including management level review of any documents posted to its websites).
9. Additionally, the CE met with each of its vendors to review the vendors' security procedures and protocols and instituted a review program, as well as reviewed its own internal procedures.
10. OCR obtained assurances that the CE and BA implemented the corrective actions listed.

Breach #622

Description:

1. Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic) has agreed to pay $750,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule by handing over protected health information (PHI) for approximately 17,300 patients to a potential business partner without first executing a business associate agreement.

2. HIPAA covered entities cannot disclose PHI to unauthorized persons, and the lack of a business associate agreement left this sensitive health information without safeguards and vulnerable to misuse or improper disclosure.

3. Raleigh Orthopaedic is a provider group practice that operates clinics and an orthopaedic surgery center in the Raleigh, North Carolina area.

4. OCR initiated its investigation of Raleigh Orthopaedic following receipt of a breach report on April 30, 2013.

5. OCR's investigation indicated that Raleigh Orthopaedic released the x-ray films and related protected health information of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films.

6. Raleigh Orthopedic failed to execute a business associate agreement with this entity prior to turning over the x-rays (and PHI).

7. "HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise," said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

8. "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected."

9. In addition to the $750,000 payment, Raleigh Orthopaedic is required to revise its policies and procedures to:

   (a) establish a process for assessing whether entities are business associates;

   (b) designate a responsible individual to ensure business associate agreements are in place prior to disclosing PHI to a business associate;

   (c) create a standard template business associate agreement;

   (d) establish a standard process for maintaining documentation of a business associate agreements for at least six (6) years beyond the date of termination of a business associate relationship; and

   (e) limit disclosures of PHI to any business associate to the minimum necessary to accomplish the purpose for which the business associate was hired.

Breach #694

Description:

1. Feinstein Institute for Medical Research (Feinstein) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR).
2. Feinstein will pay $3.9 million and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program; an effort it has already begun.
3. "Research institutions subject to HIPAA must be held to the same compliance standards as all other HIPAA-covered entities," said OCR Director Jocelyn Samuels.
4. "For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure."
5. Feinstein is a biomedical research institute that is organized as a New York not-for-profit corporation and is sponsored by Northwell Health, Inc., formerly known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty one hospitals and over 450 patient facilities and physician practices.
6. After receiving a breach notification from Feinstein involving unsecured electronic protected health information (ePHI), OCR initiated an investigation to ascertain the entity's compliance with HIPAA Rules. item OCR's investigation indicated that the following occurred:
   (a) Feinstein impermissibly disclosed the ePHI of 13,000 individuals when an Feinstein-owned laptop computer containing ePHI was left unsecured in the back seat of an employee's car;
   (b) Feinstein failed to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI held by Feinstein, including the ePHI on the aforementioned laptop computer;
   (c) Feinstein failed to implement policies and procedures for granting access to ePHI by its workforce members;
   (d) Feinstein failed to implement physical safeguards for a laptop that contained ePHI to restrict access to unauthorized users;
   (e) Feinstein failed to implement policies and procedures that govern receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility; and,
   (f) Feinstein failed to implement a mechanism to encrypt ePHI or, alternatively, document why encryption was not reasonable and appropriate and implement an equivalent alternative measure to encryption to safeguard ePHI.
7. The settlement requires Feinstein to establish a comprehensive compliance program designed to protect the security, confidentiality, and integrity of ePHI that includes:
   (a) A risk analysis and a risk management plan;
   (b) A process to evaluate and address any environmental or operational changes that affect the security of the ePHI it holds;
   (c) Policies and procedures to facilitate compliance with requirements of the HIPAA Rules;
   (d) A training program covering the requirements of the Privacy, Security, and Breach Notification Rules, intended to be used for all members of the workforce.

Breach #717

Description:

1. OCR opened an investigation of the covered entity (CE), Titus Regional Medical Center, after it reported that its EMS laptop computer that contained the protected health information (PHI) of 5,840 patients was missing upon returning from the EMS's last transport to Titus.
2. It is thought that the laptop was left on the fender of the vehicle and fell off.
3. Although the laptop was encrypted, the CE could not confirm if the laptop was opened or closed when it dropped from the vehicle.
4. If the laptop was open when it dropped, then patients' PHI (names, social security numbers, addresses, and dates of birth) may have been accessible to others.
5. The CE proved breach notification to HHS, affected individuals, and the media.
6. Following the breach the CE conducted an internal audit and determined that there was a glitch in the software parameter that permitted the download and storage of all 5,840 patients' records on the laptops regardless of the parameter setting.
7. As a result of OCR's investigation the settings on the laptops were changed, including a reduction in the time for automatic shut-off when laptops are not in use.
8. The CE applied sanctions to the EMT personnel involved and re-trained them on its privacy policies.
9. In November 2013, the CE conducted a system wide risk analysis that included all of its systems and revised and implemented its security policies.

Breach #726

Description:

1. The covered entity (CE), South Carolina Department of Health and Human Services, discovered that an employee sent Medicaid reports to her personal email from January 31, 2012, through April 4, 2012.
2. The breach affected 228,435 individuals and the types of protected health information (PHI) involved in the breach included names, addresses, phone numbers, social security numbers and for 22,648 individuals, their Medicaid identification numbers.
3. The CE provided timely breach notification to HHS, affected individuals, and the media.
4. CE also posted notification about the breach on its website.
5. In response to the breach, CE suspended access to most of its ad hoc electronic reporting, initiated a comprehensive review of its privacy and security safeguards, contacted local and federal law enforcement, and sanctioned the responsible employee.
6. The CE also revised its security policies to restrict employee access to PHI to only that necessary for the individual's job function and implemented an automated monitoring system to track user activity in its computer system.
7. CE also implemented annual privacy and security training.
8. OCR obtained assurances that the CE implemented the corrective actions listed above.

Breach #730

Description:

1. Memorial Healthcare System (MHS) has paid the U.S. Department of Health and Human Services (HHS) $5.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and agreed to implement a robust corrective action plan.

2. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area.

3. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

4. MHS reported to the HHS Office for Civil Rights (OCR) that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff.

5. This information consisted of the affected individuals' names, dates of birth, and social security numbers.

6. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals.

7. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules.

8. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

9. "Access to ePHI must be provided only to authorized users, including affiliated physician office staff" said Robinsue Frohboese, Acting Director, HHS Office for Civil Rights.

10. "Further, organizations must implement audit controls and review audit logs regularly.

11. As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen."

Breach #746

Description:

1. Anchorage Community Mental Health Services (ACMHS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule with the Department of Health and Human Services (HHS), Office for Civil Rights (OCR).
2. ACMHS will pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program.
3. ACMHS is a five-facility, nonprofit organization providing behavioral health care services to children, adults, and families in Anchorage, Alaska.
4. OCR opened an investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals due to malware compromising the security of its information technology resources.
5. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed.
6. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.
7. "Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis," said OCR Director Jocelyn Samuels.
8. "This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."
9. ACMHS cooperated with OCR throughout its investigation and has been responsive to technical assistance provided to date.
10. In addition to the $150,000 settlement amount, the agreement includes a corrective action plan and requires ACMHS to report on the state of its compliance to OCR for a two-year period.
11. The Resolution Agreement can be found on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

Breach #756

Description:

1. The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the lack of a security management process to safeguard electronic protected health information (ePHI).

2. Metro Community Provider Network (MCPN), a federally-qualified health center (FQHC), has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $400,000 and implementing a corrective action plan.

3. With this settlement amount, OCR considered MCPN's status as a FQHC when balancing the significance of the violation with MCPN's ability to maintain sufficient financial standing to ensure the provision of ongoing patient care.

4. MCPN provides primary medical care, dental care, pharmacies, social work, and behavioral health care services throughout the greater Denver, Colorado metropolitan area to approximately 43,000 patients per year, a large majority of whom have incomes at or below the poverty level.

5. On January 27, 2012, MCPN filed a breach report with OCR indicating that a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI through a phishing incident.

6. OCR's investigation revealed that MCPN took necessary corrective action related to the phishing incident;

7. however, the investigation also revealed that MCPN failed to conduct a risk analysis until mid-February 2012.

8. Prior to the breach incident, MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment, and, consequently, had not implemented any corresponding risk management plans to address the risks and vulnerabilities identified in a risk analysis.

9. When MCPN finally conducted a risk analysis, that risk analysis, as well as all subsequent risk analyses, were insufficient to meet the requirements of the Security Rule.

10. "Patients seeking health care trust that their providers will safeguard and protect their health information," said OCR Director Roger Severino.

11. "Compliance with the HIPAA Security Rule helps covered entities meet this important obligation to their patient communities."

12. The Resolution Agreement and Corrective Action Plan may be found on the OCR website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/MCPN

Breach #777

Description:

1. Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules with the Department of Health and Human Services, agreeing to a $150,000 payment.

2. APDerm will also be required to implement a corrective action plan to correct deficiencies in its HIPAA compliance program.

3. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire.

4. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

5. The HHS Office for Civil Rights (OCR) opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members.

6. The thumb drive was never recovered.

7. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process.

8. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

9. "As we say in health care, an ounce of prevention is worth a pound of cure," said OCR Director Leon Rodriguez.

10. "That is what a good risk management process is all about: identifying and mitigating the risk before a bad thing happens.

11. Covered entities of all sizes need to give priority to securing electronic protected health information."

12. In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring APDerm to develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities, as well as to provide an implementation report to OCR.

Breach #783

Description:

1. North Memorial Health Care of Minnesota has agreed to pay $1,550,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to enter into a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information.

2. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities.

3. "Two major cornerstones of the HIPAA Rules were overlooked by this entity," said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

4. "Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure."

5. OCR initiated its investigation of North Memorial following receipt of a breach report on September 27, 2011, which indicated that an unencrypted, password-protected laptop was stolen from a business associate's workforce member's locked vehicle, impacting the electronic protected health information (ePHI) of 9,497 individuals.

6. OCR's investigation indicated that North Memorial failed to have in place a business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf.

7. North Memorial gave its business associate, Accretive Health, Inc., access to North Memorial's hospital database, which stored the ePHI of 289,904 patients.

8. Accretive also received access to non-electronic protected health information as it performed services on-site at North Memorial.

9. The investigation further determined that North Memorial failed to complete a risk analysis to address all of the potential risks and vulnerabilities to the ePHI that it maintained, accessed, or transmitted across its entire IT infrastructure – including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

10. In addition to the $1,550,000 payment, North Memorial is required to develop an organization-wide risk analysis and risk management plan, as required under the Security Rule.

11. North Memorial will also train appropriate workforce members on all policies and procedures newly developed or revised pursuant to this corrective action plan.

Breach #784

Description:

1. A box containing 2,600 paper records of tissue implants used in surgeries was discarded by a waste disposal contractor of the covered entity (CE), NYU Hospital for Joint Diseases Inventory Management Department, when the box was not property secured.
2. The box contained the protected health information (PHI) of 2,239 individuals and included names, dates of birth, dates of surgery, surgeon names, procedures, and types and serial numbers of the tissues used in the surgeries.
3. Upon discovery of the breach, the CE contacted the waste disposal contractor and determined that the documents were discarded and buried in a landfill out of state.
4. The CE provided breach notification to HHS, the media, and affected individuals, and posted substitute notice on its website.
5. As a result of OCR's investigation, the CE improved safeguards by storing all tissue records in a locked cabinet and requiring management to store the keys.
6. In addition, the CE counseled the employees involved in the incident and retrained all staff on its policies and procedures for safeguarding PHI.
7. The CE also implemented a plan to conduct reviews of HIPAA compliance, including both physical access and physical security risks.

Breach #807

Description:

1. On March 22, 2011, during a house raid, the Secret Service discovered the protected health information (PHI) of approximately 880 patients of the covered entity (CE), Troy Regional Medical Center, in the form of admission "face sheets."
2. The PHI involved in the breach included demographic information, such as patients' names, dates of birth, social security numbers, and medical record numbers.
3. The CE could not accurately identify the person responsible for breaching its electronic medical record (EMR) system due to a software error which erroneously recorded multiple occasions of systems access when workforce members were accessing the system for legitimate business purposes.
4. Due to this software error, the CE could not effectively assist in the criminal investigation being conducted by local law enforcement and the Secret Service.
5. The CE provided breach notification to HHS, the media, and affected individuals and posted substitute notice on its website.
6. It also provided a toll-free information number and offered credit monitoring for one year.
7. In response to the incident, the CE worked with its IT vendor to increase data security monitoring and implement automatic log-out for its EMR system.
8. The CE also updated and added to its policies and procedures, improved system review documentation, implemented verification of user access rights, and developed sample audit logs.
9. The CE also retrained employees on its HIPAA security policies.
10. OCR obtained assurances that the corrective actions listed above were completed.

Breach #818

Description:

1. Thieves broke into the PMC Medicare Choice facility located in Humacao, Puerto Rico and stole four unencrypted desktop computers containing 24,361 health plan members' electronic protected health information (ePHI).
2. The ePHI included names, addresses, phone numbers, Medicare HIC numbers, diagnosis and treatment information, health plan names, health plan member identification numbers, health plan enrollment information, health care claim information, and social security numbers.
3. The covered entity (CE) provided breach notification to HHS, affected individuals, and the media.
4. Following the breach, the CE repaired a damaged wall and improved security at the facility and the surrounding premises.
5. OCR obtained assurances that the CE implemented the corrective actions noted above.
6. As a result of OCR's investigation, the CE encrypted all computers located at its regional offices.
7. OCR stated its expectation that the CE will perform a thorough and accurate risk analysis and establish a risk management plan.
8. In addition, OCR stated an expectation that the CE will implement contingency operations procedures, implement its facility security plan's policies and procedures, and regularly patch and update its IT infrastructure.
9. OCR also stated an expectation that the CE will encrypt and decrypt ePHI where appropriate and document the technical safeguards implemented to prohibit the unauthorized copying and removal of PHI and ePHI.

Breach #826

Description:

1. A workforce member of the covered entity's (CE) business associate (BA) saved the electronic protected health information (ePHI) of approximately 93,500 patients on an unsecured computer drive in order to do work from home, and subsequently lost the hard drive.
2. The PHI included names, addresses, dates of birth, marital status, social security numbers and medical record numbers.
3. Following the breach, the workforce member involved was sanctioned for violating the CE's policies.
4. The CE provided breach notification to the media, HHS, and all affected individuals.
5. It also offered all affected individuals 2 years of free identity protection services.
6. In addition, the CE disabled the ability for all of its computing devices to download ePHI via USB connection ports.
7. Further, it began implementing malicious software prevention utilities as well as data encryption controls to supplement its portable computing devices.
8. OCR obtained assurances that the CE implemented the corrective action listed above.
9. The breach incident involved a BA and occurred prior to the September 23, 2013, compliance date.
10. OCR verified that the CE had a proper BA agreement in place that restricted the BA's use and disclosure of PHI and required the BA to safeguard all PHI.

Breach #861

Description:

1. Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network.
2. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.
3. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.
4. NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP.
5. NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities.
6. The shared network links to NYP patient information systems containing ePHI.
7. The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI.
8. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines.
9. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.
10. In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections.
11. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI.
12. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI.
13. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.
14. "When entities participate in joint compliance arrangements, they share the burden of addressing the risks to protected health information," said Christina Heide, Acting Deputy Director of Health Information Privacy for OCR.
15. "Our cases against NYP and CU should remind health care organizations of the need to make data security central to how they manage their information systems."
16. NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.

Breach #904

Description:

1. A car containing an unencrypted laptop computer was stolen from West Monroe Partners, a contractor for the covered entity's (CE) business associate (BA), DentaQuest.
2. The laptop stored a database containing the electronic protected health information (ePHI) of approximately 76,000 individuals, including data on 10,515 of the CE's members.
3. The types of PHI involved in the breach included names, social security numbers, dates, and certain provider identification numbers.
4. The CE and BA worked together to provide breach notification to affected individuals and the media, and offered free credit monitoring and enhanced credit services to affected individuals for one year.
5. The CE reported the breach to HHS and provided substitute notification on its website.
6. The BA implemented procedures to ensure that any third party laptops connecting to its network employ disk encryption.
7. Further, the BA established a policy to prohibit contractors from storing PHI on laptops.
8. The breach incident involved a BA and occurred prior to the September 23, 2013, compliance date.
9. OCR verified that the CE had a proper BA agreement in place that restricted the BA's use and disclosure of PHI and required the BA to safeguard all PHI.

Breach #907

Description:

1. The covered entity's business associate (BA), Siemens Medical Solutions USA, Inc., shipped seven unencrypted compact disks (CDs) that contained the electronic protected health information (ePHI) of 130,495 individuals to the covered entity (CE), Lincoln Medical and Mental Health Center.
2. The CD's, containing back-up data, were lost in transit.
3. The ePHI included names, addresses, social security numbers, medical record numbers, health plan information, dates of birth, dates of admission and discharge, diagnostic and procedural codes, and driver's license numbers.
4. The CE provided breach notification to affected individuals, HHS, and the media.
5. Upon discovery of the breach, the CE directed the BA to cease using the shipping service as a means of transporting the CDs.
6. As a result of OCR's investigation, the BA adopted a procedure to encrypt CDs.
7. The CE also implemented a procedure for a senior employee of the BA to physically deliver the encrypted CDs to the CE.
8. The breach incident involved a BA and occurred prior to the September 23, 2013, compliance date.
9. OCR verified that the CE had a proper BA agreement in place that restricted the BA's use and disclosure of PHI and required the BA to safeguard all PHI.

Breach #913

Description:

1. The covered entity (CE), University of Rochester Medical Center and Affiliates, reported that on April 19, 2010, 2,628 patient billing statements for Strong Memorial Hospital were sent to the wrong patients.

2. The statements contained patients' names, addresses, guarantors' names, guarantors' addresses, dollar amounts owed, health insurance plans, subscriber numbers, social security numbers, general descriptions of services rendered (such as inpatient room charge, outpatient visit charge, physical therapy, laboratory, pharmacy, radiology, etc.) and dates of service.

3. The CE provided breach notification to HHS, affected individuals, and the media.

4. As a result of the breach, the CE established a numerical counter to ensure that the numbers of statements that run through the folding machine are matching the numbers of statements that are printing.

5. In addition, a report was added to the statement bundles distributed by the printing center that identifies the number of pages printed for each statement run.

6. Further, a quality control process was put into place where a second staff member manually inspects stuffed envelopes on a random basis to ensure that the correct number of pages are inserted as well as verifying that the contents are all for the same patient.

7. As a result of OCR investigation, OCR reviewed a copy of the CE's risk assessment and policies and procedures relating to uses and disclosures of protected health information (PHI) and safeguarding PHI.

Breach #926

Description:

1. Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity Health Plan, Inc. will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules for $1,215,780.

2. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area.

3. Affinity filed a breach report with the HHS Office for Civil Rights (OCR) on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act.

4. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information.

5. Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity.

6. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

7. Affinity estimated that up to 344,579 individuals may have been affected by this breach.

8. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives.

9. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

10. "This settlement illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent," said OCR Director Leon Rodriguez.

11. "HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information."

12. In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all ePHI.

Breach #934

Description:

1. An employee's car was broken into and a tote bag, which had a paper spreadsheet containing protected health information (PHI), was stolen.
2. The spreadsheet contained PHI pertaining to 554 patients and included patients' names, ages, weight, race, social security numbers, and blood and tissue typing.
3. The covered entity (CE), North Carolina Baptist Hospital, provided breach notification to HHS, affected individuals, and the media, and offered affected individuals a year of credit monitoring services along with a toll-free number to contact.
4. Following the breach, the CE reviewed the applicable policies and procedures with the clinic responsible, revised the spreadsheet to no longer include patients' social security numbers, and counseled and warned the involved employee about the requirements for properly safeguarding PHI.
5. Additionally, the Chief Executive Officer of the Medical Center emailed all employees to re-educate them about the importance of properly safeguarding PHI and the expectations for compliance and commitment to adhering to federal and state privacy and security laws.
6. As a result of OCR's investigation, the CE provided an alternate, secure way to electronically access the clinic spreadsheet, installed video cameras in the parking dock, and externally inspected employee vehicles to assure no PHI was visible.
7. The CE established a Privacy and Information Security Council to help identify ways to improve and strengthen privacy and security policies and practices.

Breach #954

Description:

1. Computer backup tapes containing EPHI for the office practice management program including electronic medical records were stolen from the home of the practice manager on December 11, 2009.
2. The breach affected approximately 1,860 patients.
3. The protected health information on the tapes contained patients' names, addresses, telephone numbers, dates of birth, insurance information, social security numbers and medical record information.
4. Following the breach, Sigman took the following voluntary corrective actions:
   (a) (1) upgraded software application for backup security;
   (b) implemented a new external backup system in case the server goes down;
   (c) (2) encryption software was implemented for data contained on both its backup tapes and network storage device;
   (d) (3) revised its security policy for transporting backup media;
   (e) backup tapes must now be stored in a lockbox within a locked office in its facility;
   (f) the revised policy also prohibits the movement of backup tapes from the facility as well as restricts access to the tapes to designated workforce;
   (g) (4) employees were retrained on the policies and procedures in place and received training on the new policies and procedures for safeguarding backup tapes;
   (h) (5) notified affected individuals and the media.

Breach #956

Description:

1. The covered entity (CE) changed the business associate (BA) it used as its information technology vendor.
2. During the transition, a workforce member of the outgoing BA entered the CE's computer system, changed the passwords, disabled all accounts, and removed drive mappings on the computer server for all of the workstations.
3. The BA also removed the CE's backup program and deactivated all of its antivirus software.
4. The breach affected approximately 2,000 individuals.
5. The protected health information (PHI) involved in the breach included patients' names, addresses, dates of birth, social security numbers, appointments, insurance information, and dental records.
6. The CE provided breach notification to affected individuals, HHS, and the media.
7. Following the breach, the CE implemented security measures in its computer system to ensure that its information technology associates do not have access to the CE's master system and enabled direct controls for the CE.
8. A new server was installed with no ties to the previous BA.
9. The new BA corrected the CE's passwords and settings, mitigating the issues caused by the previous vendor.
10. The CE provided OCR with copies of its HIPAA security and privacy policies and procedures, and its signed BA agreements that included the appropriate HIPAA assurances required by the Security Rule.
11. As a result of OCR's investigation, the CE improved its physical safeguards and retrained employees.

Breach #957

Description:

1. In its breach report and during the course of OCR's investigation, the covered entity advised that it took various corrective actions to prevent a reoccurrence of the breach.
2. Specifically, the covered entity conducted a risk assessment which revealed that the breach posed a significant risk of financial, reputational, or other harm to the 83,000 members.
3. The covered entity sent notification letters to 83,000 members apologizing for the breach and offered a year of free credit monitoring and a $25,000 insurance policy against identity theft ($10,000 for New York residents).
4. The covered entity also provided training to its call centers on November 29, 2009 to answer inquiries from callers concerned about the breach.
5. In addition, media outlets were contacted to alert of a breach in states in which more than 500 members were impacted by the breach.
6. The covered entity advised that media outlets were identified based on location of membership impacted, as well as ensuring it was a major media outlet and press releases were sent to 21 major media outlets on December 18, 2009.
7. The covered entity also created and implemented a new policy titled 'Personal Health Information and Personal Identifiable Information Data Security and Handling Policy Acknowledgement Form' that centralized all data requests through a 'Team Track' which is an internal electronic submission request that ensures all PHI requested data receives the sign off of the Privacy Officer and Security Officer prior to release.
8. Further, the covered entity also provided a mandatory annual computer-based training to all staff in May 2010.