PHI Breaches for Anthem, Inc.

Incident Month/ Year	Type of Breach	Number of Individuals Affected	Description/Safeguards Prior to Breach	Actions Taken in Response to Breach
4/2019	Hacking/IT Incident	185	A person impersonating an employee of a provider called the Web Support Help Desk. The impersonator was able to provide enough information about the log-on credentials of the employee to gain access to the provider portal.	Implemented new technical safeguards; Revised policies and procedures Trained or retrained workforce members.
1/2019	Hacking/IT Incident	54,528	Unauthorized persons gained access to a vendor's email accounts. The incident was caused by a phishing attack on the vendor's systems.	Changed password/strengthened password requirements; Implemented new technical safeguards; Provided business associate with additional training on HIPAA requirements; Provided individuals with free credit monitoring; Revised policies and procedures; Took steps to mitigate harm.
12/2018	Unauthorized Access/Disclosure	1	Correspondence was sent to wrong recipient.	Sanctioned workforce members involved (including termination); Trained or retrained workforce members; Took steps to mitigate harm.
11/2018	Unauthorized Access/Disclosure	1	Vendor employee entered the wrong address when updating a member's address in the system, resulting in correspondence being sent to a provider's address.	Sanctioned workforce members involved (including termination); Trained or retrained workforce members; Took steps to mitigate harm.
10/2018	Hacking/IT Incident	43	Business associate's vendor had an employee whose credentials were compromised exposing our member's data.	Implemented new technical safeguards; Took steps to mitigate harm; Trained or retrained workforce members; Other - The employee's password was immediately changed. The vendor hired a third party forensic firm to complete an independent and comprehensive investigation that confirmed no other compromise of their system, and identified additional safeguard to be implemented to further limit the access to patient information. Vendor employees were retrained on information security.
10/2018	Unauthorized Access/Disclosure	315	Vendor issue that impacted a page break formatting issue with Pharmacy Prior Authorization letters caused PHI disclosures.	Sanctioned workforce members involved (including termination); Trained or retrained workforce members; Took Steps to Mitigate harm.
9/2018	Unauthorized Access/Disclosure	1	Vendor made a system coding change that impacted our membership files.	Implemented new technical safeguards; Took steps to mitigate harm.
8/2018	Unauthorized Access/Disclosure	1	System error caused one member to view another member's information on web portal.	Took steps to mitigate harm; Revised policies and procedures; Implemented new technical safeguards.

Incident Month/ Year	Type of Breach	Number of Individuals Affected	Description/Safeguards Prior to Breach	Actions Taken in Response to Breach
8/2018	Unauthorized Access/Disclosure	1	Business associate generated an authorization using the wrong address. This caused a member's information to be disclosed to the wrong recipient.	Corrected data in system and retrained employee.
7/2018	Unauthorized Access/Disclosure	1	Employee mistakenly sent an email to a member instead of an internal employee.	Sanctioned workforce members involved (including termination); Trained or retrained workforce members; Took steps to mitigate harm.
7/2018	Unauthorized Access/Disclosure	1	Employee sent correspondence to a member that included another member's PHI.	Sanctioned workforce members (including termination); Trained or retrained workforce members; Took steps to mitigate harm.
6/2018	Hacking/IT Incident	462	External broker's email account was compromised by an unauthorized individual.	Implemented new technical safeguards; Trained or retrained workforce members; Took steps to mitigate harm.
6/2018	Unauthorized Access/Disclosure	2	Wrong provider address was given to vendor to send letters resulting in letters being sent to the wrong address.	Took steps to mitigate harm.
2/2018	Unauthorized Access/Disclosure	1	Information was viewable by another member when logging into the online web portal	Online account disabled, Revised Internal Procedure/Policy.
10/2017	Unauthorized Access/Disclosure	11	Employee made an error that resulted in correspondence being sent to the wrong recipient.	Revised policies and procedures; Sanctioned workforce members involved (including termination); Trained or retrained workforce members.
9/2017	Unauthorized Access/Disclosure	3	Business associate addressed letters including information that should not have appeared on the envelopes and mailed them out.	Provided individuals with free credit monitoring, Revised policies and procedures, Sanctioned workforce members involved (including termination), Trained or retrained workforce members Under the Freedom of Information Act and HHS regulations.
8/2017	Unauthorized Access/Disclosure	171	Business associate posted applicant information to an unsecured server.	Provided business associate with additional training on HIPAA requirements; Revised policies and procedures.
7/2017	Unauthorized Access/Disclosure	18,500	Business associate reported that an employee was likely involved in identity theft related activities. Upon investigating, the business associate learned the employee emailed a file with information about members to their personal email address on July 8, 2016.	Created a new/updated Security Rule Risk Management Plan; Implemented new technical safeguards; Performed a new/updated Security Rule Risk Analysis; Provided business associate with additional training on HIPAA requirements; Provided individuals with free credit monitoring; Sanctioned workforce members involved (including termination); Took steps to mitigate harm.
7/2017	Unauthorized Access/Disclosure	1	Business associate's employee made an error that resulted in correspondence being sent to the wrong recipient.	Sanctioned workforce members involved (including termination); Took steps to mitigate harm.

Incident Month/ Year	Type of Breach	Number of Individuals Affected	Description/Safeguards Prior to Breach	Actions Taken in Response to Breach
7/2017	Unauthorized Access/Disclosure	1	Business associate experienced a system error that resulted in information being seen by the wrong recipient.	Revised policies and procedures; Took steps to mitigate harm.
6/2017	Unauthorized Access/Disclosure	131	A business associate's employee verified address information incorrectly which caused correspondence to be sent to the incorrect recipient.	Provided individuals with free credit monitoring; Revised policies and procedures.
9/2016	Unauthorized Access/Disclosure	3,525	Learned on September 1, 2016 that an individual in the sales department emailed company information to his personal email address between February and September of this year. His actions violated policies on the accessing and handling of protected health information and personally identifiable information. The information emailed included certain elements of personal information, including names, dates of birth, addresses, health plan, information and, in some cases, Medicare ID numbers.	Provided individuals with free credit monitoring; Revised business associate contracts; Revised policies and procedures; Sanctioned workforce members involved (including termination); Took steps to mitigate harm; Trained or retained workforce members; Directed the individual to securely destroy the information that was not properly in his possession and took steps to confirm the destruction.
12/2015	Unauthorized Access/Disclosure	499	Business associate sent correspondence to the wrong recipients.	Took steps to mitigate harm; trained or retrained workforce members.
11/2015	Unauthorized Access/Disclosure	1	Our employee set up a case for mental health in the system under the wrong member. This led to information being disclosed to the wrong recipient.	Corrected data in system. Associate sanctioned and retrained.
4/2015	Unauthorized Access/Disclosure	1	Our employee attached the wrong document to an email, which included PHI that was not intended for the recipient.	Revised policies and procedures; Sanctioned workforce members involved (including termination).
3/2015	Unauthorized Access/Disclosure	268	Due to a system error, subrogation questionnaires were sent to old addresses instead of the current subscriber address, causing correspondence to be sent to the wrong recipient.	Steps were taken to mitigate harm including notifying impacted members and putting in place a system fix which solved the issue.

Incident Month/ Year	Type of Breach	Number of Individuals Affected	Description/Safeguards Prior to Breach	Actions Taken in Response to Breach
1/2015	Hacking/IT Incident	78,800,000	January 2015, Anthem, Inc. discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Anthem, Inc.'s IT system and obtained personal information relating to consumers who were or are currently covered by Anthem, Inc. or other independent Blue Cross and Blue Shield plans that work with Anthem, Inc. These cyber attackers gained unauthorized access to Anthem, Inc.'s IT system and obtained personal information from individuals such as their names, birthdays, member identification (ID) and/or Social Security numbers, street addresses, email addresses and employment information.	Created a new/updated Security Rule Risk Management Plan; Implemented new technical safeguards; Performed a new/updated Security Rule Risk Analysis; Provided business associate with additional training on HIPAA requirements; Provided individuals with free credit monitoring; Sanctioned workforce members involved (including termination); Took steps to mitigate harm; Changed password/strengthened password requirements; Implemented new technical safeguards; Provided individuals with free credit monitoring; Took steps to mitigate harm; Trained or retrained workforce members.