Problems at Planned Parenthood

Information for Protecting Our Health

The website includes many individual complaints listed under the specific locations at which they occurred. They're not re-iterated here.

Our website, organized by locations, is constantly updated. It also includes documentation of health inspection reports, malpractice suits, 911 calls, and cases involving sexual abuse, racism or financial ethics:

www.problemsatplannedparentood.org

United States

	You scheduled an abortion. Planned Parenthood's website could tell Facebook. The organization left marketing trackers running on its scheduling pages by Tatum Hunter, *The Washington Post*, June 29, 2022

California

Los Angeles

	400,000 Patients Potentially Affected by Planned Parenthood Ransomware Attack by Steve Alder. *The HIPPA Journal,* December 3, 2021

	Planned Parenthood Los Angeles Settles Class Action Data Breach Lawsuit for $6 Million by Steve Alder. *The HIPPA Journal,* April 8, 2024

Court Complaints for a class action lawsuit were originally filed separately from:

- *A.K.,*
- *Danchick,*
- *Garza,*
- *Jane Doe,*
- *K.O.*
- *Orellana*
- Pawlukiewicz
- *T.S.*

The full documents are at

www.problemsatplannedparenthood.org/california-los-angeles

San Jose

Balli

The 2022 Complaint is at:

www.problemsatplannedparenthood.org/california-san-jose

22. Defendants hired Plaintiff as VoIP Architect on October 7, 2019. Plaintiff was hired with more than 20 years of relevant work experience. Plaintiff's work responsibilities included . . . general information technology responsibilities, ensuring data security . . .

32. On or about November 15, 2019, Plaintiff learned that Defendants had experienced a serious data breach which had exposed confidential and private Personal Health Information ("PHI") protected by . . . (HIPPA). Plaintiff immediately reported the breach to [J.L.] Plaintiff reported that the PHI of hundreds of individuals had been unlawfully disclosed . . . [and] that the breach needed to be addressed as soon as possible . . . [and] that Defendants were required to inform the Company's Ethics and Compliance Department and the State of California about the PHI data breach.

33. [J.L.] stated that she could not take any steps to address or remedy the PHI data breach because doing so would risk PPMM's accreditation status with parent entity Planned Parenthood Federation of American. Plaintiff nonetheless continued to insisted that the PHI data breach be reported to the proper authorities and remedied according to applicable regulations.

34. [J.L.] became agitated and ordered Plaintiff not to discuss the PHI data breach with any other individual. She threatened Plaintiff and told him that if he disobeyed her instruction his employment with Defendants would be terminated.

35. Plaintiff believed that Defendants PHI data breach needed to be further reported and remedied. Initially, however, he complied with [J.L]'s orders because he relied upon the income from his employment with Defendants to support himself and his family.

36. On or about January 28, 2020, Plaintiff reported the November 2019 PHI data breach to the Company's Interim General Counsel and Chief Compliance Officer . .

38. Plaintiff further reported to [her] that Defendants were poised to expose additional HIPAA-protected PHI due to the compromised nature of Defendant's network infrastructure.

39. [She] told Plaintiff that the Company had made multiple mistakes . . . [and] thanked Plaintiff for reporting the data breach and assured him that there would be no retaliation for his actions.

40. The very next day, January 29, 2020, Defendants revoked Plaintiff's information technology (IT) account rights so that he could not perform his job duties. Defendants' Human Resources department informed Plaintiff that he was being suspended form work effective immediately. Plaintiff surrendered his work laptop, keys, and security badge.

Delaware

Wilmington

Testimony at a Delaware legislative hearing, July 20, 2013
Melody Meanor, the former Health Center Manager of Family Planning at Planned Parenthood of Delaware in Wilmington

One area I attempted to correct was inadequate protection of patient confidentiality and privacy. At the beginning of my employment, I struggled to correct negative patient care violations that involved HIPAA violations. Untrained health center assistants simply did not understand the importance of protecting patient privacy. My attempts to train and discipline health center assistants were significantly undermined… The Medical Director . . . should have put a stop to these sorts of behaviors. However, at the same time as she was serving as the Medical Director of Planned Parenthood of Delaware, [she] was simultaneously employed by the Planned Parenthood Federation of America as an auditor inspecting other Planned Parenthood affiliates.

Iowa

Dubuque

	Planned Parenthood leaves records in Dubuque; info of 2,500 potentially exposed by Jeff Montgomery, July 6, 2016

Excerpt:

About 2,500 patients of Planned Parenthood of the Heartland's now-closed Dubuque center recently were notified that their health records might have been among those left behind when the facility closed in April.

Public Relations Manager Rachel Lopez said hard copies of patient information were inadvertently left at the building at 3365 Hillcrest Road and that they might have been accessed by unauthorized parties following the center's closure and ensuing building sale. . .

The documents were found by the building's new owner May 6. Lopez said Planned Parenthood sent letters to all affected patients Friday, July 1 — nearly two months after the discovery . . .

Executive Director Kris Nauman said the documents were discovered during a May 6 final walk-through at the facility. Clarity Clinic closed on the building purchase later that day.

The medical information was located in a closet in "copy paper boxes" that were not sealed, she said.

Montana

Documents for both class action lawsuits are at:

www.problemsatplannedparenthood.org/montana

Downey

6. The impact to its systems strongly implies that Defendant lacked sufficient cybersecurity incident response and disaster recovery plans . . . as is the industry norm.

7. Notwithstanding that the attack occurred at least by August 24, 2024, Defendant waited until November 5, 2024, to begin notifying its current and former patients of the Data Breach.

8. Defendant's unreasonable and unexplained delays prevented Plaintiff from being able to timely protect herself from the significantly increased risk of harm . . .

78. Because of the Data Breach, Plaintiff Downey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach . . . Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Sullivan

2. The Private Information compromised in the Data Breach included certain personal or protected health information . . . including Plaintiff's minor child . . .

3. The Private Information was exposed to cybercriminals who perpetrated the attack and remains in the hands of those cybercriminals. According to Defendant's report to the U.S. Department of Health and Human Services, 18,003 individuals' sensitive data was compromised . . .

32. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay in in *no case later that 60 calendar days* from the discovery of the breach." . . .

34. Defendant's notice to HHS was dated November 5, 2024 – around ten weeks after the incident was discovered.

35. Defendant had obligations created by HIPPA, contract, industry standards, state statutes, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

New York

Huntington

Curtis

The 2008 Complaint is under Huntington:

www.problemsatplannedparenthood.org/new-york

Excerpt:

29. That on the 7th day of June, 2007, the plaintiff . . . underwent surgical procedures of **a** highly personal, privileged, private and confidential nature by the defendant . . .

32. That at all times herein mentioned . . . the Defendant failed, neglected and or omitted to properly and adequately . . . ensure the appropriate . . . protocols with respect to said covenant of patient confidentiality . . .

39. That the foregoing unauthorized disclosure . . . was performed in such a careless . . . and willful manner as to manifest . . . a reckless disregard for the rights, health and well-being of the plaintiff . . .

44. That . . . this plaintiff was severely injured and damaged, rendered sick, sore, lame and disabled, sustained severe nervous shock and mental anguish, great pain and emotional upset, some of which injuries are permanent . . . and plaintiff will be permanently caused to suffer pain . . . plaintiff incurred and in the future will necessarily incur further hospital and/or medical expenses in an effort to be cured of said injuries . . . and plaintiff will be unable to pursue the usual duties with the same degree of efficiency as prior to the negligence and breach of fiduciary duty and covenant of confidentiality on the part of the defendant, all to plaintiff's great damage.

Note: This lengthy and repetitive document never does have an explanation as to how the breach of confidentiality occurred nor how it led to the medical problems.

Ohio

Cincinnati

Documents are under Cincinnati:

www.problemsatplannedparenthood.org/ohio

Excerpt from the letter of the Office of Civil Rights:

On October 1, 2014, the Covered Entity (CE) mistakenly disposed of binders containing protected health information (PHI). The CE's archived prescription dispensing logs and waived lab test logs were left in an unlocked closet after business hours and a custodian mistakenly put them in a trash dumpster. The following morning, the dumpster was emptied by the trash collector who took it to be buried with other garbage at a landfill that same day. The PHI involved in the incident included the names, dates of birth, lab results, and medications of approximately 5,000 individuals. After the CE filed the breach report, it determined that the incident was a nonreportable breach based on a four part breach assessment and a low probability that the PHI in the binders had been compromised.

Cleveland

Doe

The 2005 Complaint is under Cleveland:

www.problemsatplannedparenthood.org/ohio

Excerpt:

4. On or about November 19, 2002, Plaintiff visited Planned Parenthood, for the purpose of receiving confidential, highly sensitive medical treatment, the details of which were recorded in Plaintiffs non-public medical record.

5. On or about July 9,2003, Plaintiff again visited an office of Planned Parenthood to receive medical treatment . . .

6. On or about the dates of July 6th through the 13th, Defendant . . . disclosed and or caused Plaintiffs treating physician to disclose highly confidential medical information about the Plaintiff to third parties without Plaintiffs consent. These third parties had no legitimate interest in receiving such information . . .

12. As a result of inducing the unauthorized disclosure of Plaintiff's non-public information, Plaintiff sustained injury in the form of damaged reputation, humiliation, emotional anguish, shame and public ridicule. Plaintiff has suffered and continues to suffer scorn, contempt, and ridicule by neighbors, family members, and others, and has lost reputation and standing in the community, all of which has caused Plaintiff humiliation, embarrassment, hurt feelings, mental anguish, pain and suffering, all to Plaintiff's damage.

Washington, D.C.

	D.C.'s Planned Parenthood reports data was breached last fall. Months later, the organization has started reaching out to affected patients and donors by Brittany Renee Mayes, *The Washington Post*, April 16, 2021

Excerpt:

On Oct. 21, the investigation determined that "unauthorized actors gained access to [the] network." It also revealed that the data breach, which occurred from Aug. 27 to Oct. 8, impacted only the D.C. branch . . . Leaked information included names, addresses, dates of birth, diagnoses, treatments and prescription information. Social Security and financial information was also included in the breach . . .

On April 9, PPMW began mailing letters to affected patients about whom they could reach for guidance on further protecting their information. The findings of the investigation found "no reason to suspect that there has been any fraudulent use of patient information associated with this incident." However, the organization is providing patients whose Social Security and driver's license numbers were compromised with complimentary credit monitoring and identity-theft protection services. Donors with compromised bank information did not receive the same service offer.