

FOR IMMEDIATE RELEASE**September 2, 2015****Contact: HHS Press Office****202-690-6344**

\$750,000 HIPAA settlement emphasizes the importance of risk analysis and device and media control policies

Cancer Care Group, P.C. 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 (HHS), Office for Civil Rights (OCR). Cancer Care paid \$750,000 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Cancer Care Group is a radiation oncology private physician practice, with 13 radiation oncologists serving hospitals and clinics throughout Indiana.

On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured electronic protected health information (ePHI) after a laptop bag was stolen from an employee's car. The bag contained the employee's computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients.

OCR's subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. It had not conducted an enterprise-wide risk analysis when the breach occurred in July 2012. Further, Cancer Care did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice within the organization. OCR found that these two issues, in particular, contributed to the breach, as an enterprise-wide risk analysis could have identified the removal of unencrypted backup media as an area of significant risk to Cancer Care's ePHI, and a comprehensive device and media control policy could have provided employees with direction in regard to their responsibilities when removing devices containing ePHI from the facility.

"Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information," said OCR Director Jocelyn Samuels. "Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information."

Cancer Care has taken corrective action with regard to the specific requirements of the Privacy and Security Rules that are at the core of this enforcement action, as well as actions to come into compliance with the other provisions of the HIPAA Rules. The Resolution Agreement and Corrective Action Plan (CAP) can be found on the OCR website at:

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cancercare.html>

HHS offers guidance on how your organization can conduct a HIPAA Risk Analysis:

<http://www.healthit.gov/providers-professionals/security-risk-assessment>

To learn more about non-discrimination and health information privacy laws, your civil rights, and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at

<http://www.hhs.gov/ocr/office>.

###

Note: All HHS press releases, fact sheets and other news materials are available at <http://www.hhs.gov/news>.

Like HHS on Facebook [↗](#), follow HHS on Twitter [@HHSgov](#) [↗](#), and sign up for HHS Email Updates.

Last revised: September 2, 2015

Sign Up for News Release Updates

Enter your email:

Submit

Public Affairs Contacts

HHS Media Information

Office of the Assistant Secretary for Public Affairs (ASPA) Contacts

HHS Operating Divisions

HHS Staff Divisions

HHS Regions