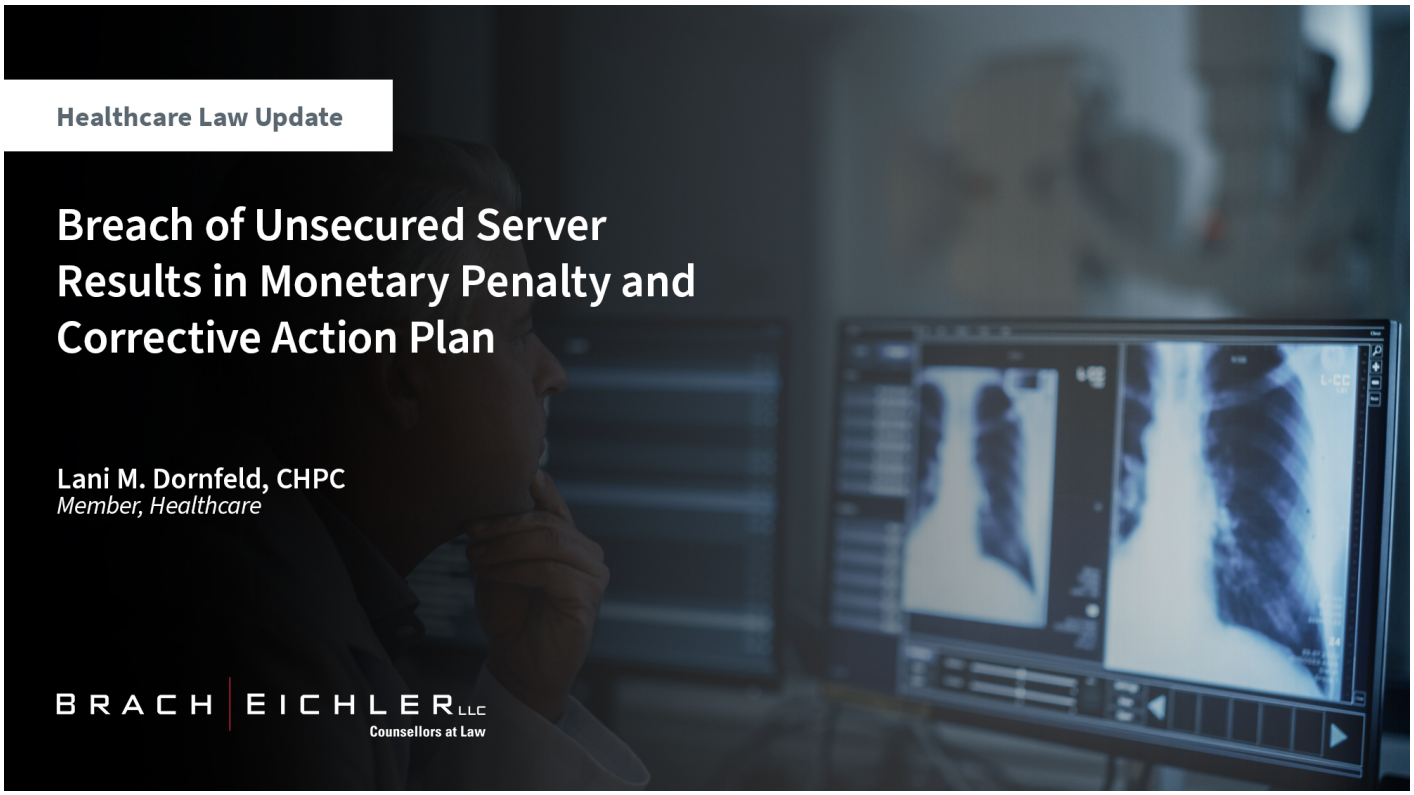
Breach of Unsecured Server Results in Monetary Penalty and Corrective Action Plan



6/1/2025

The U.S. Department of Health and Human Services (DHHS) recently entered into a Resolution Agreement with an imaging provider relating to the breach of a picture and archiving communications system (PACS) server containing medical images of its patients. The investigation of the provider was initiated by the DHHS Office for Civil Rights (OCR) after OCR obtained information alleging that protected health information maintained or stored by the provider was accessible via the internet and disclosed as the result of an unsecure PACS server. Per the Resolution Agreement, the investigation revealed that the provider "never conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information that it holds," as required by the HIPAA Security Rule, and the provider "failed to notify affected individuals of a breach within 60 days of discovery of the breach," as required by the HIPAA Breach Notification Rule.

Although the penalty of $25,000 assessed by DHHS is relatively low, the Resolution Agreement contains a number of corrective action obligations the provider must undertake, including, but not limited to, (i) sending breach notification to the affected individuals, the media and DHHS; (ii) conducting a complete and accurate risk assessment of the provider's systems, with the scope and methodology of such risk assessment pre-approved by DHHS; (iii) conducting annual risk assessments; (iv) developing risk management plans based on the results of the risk assessments; (v) developing and revising the provider's HIPAA policies and procedures and submitting them to DHHS for review and approval; (vi) distributing the final policies and procedures to the provider's workforce and obtaining compliance certifications; (vii) training workforce members; and (viii) submitting an implementation report and annual reports to DHHS during the corrective action period.

The resolution of this breach event demonstrates that, although there is a financial and human resources cost to proper and full implementation of the requirements of HIPAA, the cost of a breach event, even one with a low monetary penalty, can be extremely high.

Click Here to read the entire June 2025 Healthcare Law Update now!

For more information or assistance with your organization's privacy and security program, contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

Authors

The following attorneys contributed to this insight.

Lani M. Dornfeld

CHPC, Member
Healthcare Law

973.403.3136 · 973.618.5536 Fax

ldornfeld@bracheichler.com