



December 10, 2008

What to Do About Stolen or Lost Records

Quick Links

[CAP Home](#)

[Risk E-Notes Archive](#)

[CAPsules Archive](#)

[CAP Risk Management
& Patient Safety](#)

[Contact Us](#)



Q: What should you do when a laptop computer with patient information or a patient medical record is stolen from your office or your provider's car?

A: The law requires patient notification when patient identifying information is unencrypted. Unencrypted information includes a patient's name, social security number, passport number, driver's license number, credit card number, or pin. The Health Insurance Portability and Accountability Act (HIPAA) requires that any breach of information, including lost or stolen information, be listed on your log of disclosures.

CAP's Risk Management & Patient Safety Department recommends that you **notify patients, by phone initially and then by letter**, when their health information or medical record has been lost or stolen.

Failure to notify the patient can lead to the following situations:

- Medical identity theft of your patient's information.
- Loss of your patient's trust.
- Loss of reputation.

Your letter to the patient should include:

- A brief description of what occurred.
- Which branch of law enforcement is involved in the investigation.
- What attempts are being made to reconstruct the record.
- Recommendations and phone numbers for reporting and placing fraud alerts on their consumer reports. Several consumer fraud agencies are: Equifax, Experian, and TransUnion.

Authored by
Ann Whitehead, RN, JD
CAP Risk Management & Patient Safety Department

If you have questions about this article, please use the "Contact Us" button to the left.

Published comments of this information should not be considered legal advice applicable to a specific situation. Legal guidance for individual matters should be obtained from a retained attorney.