

CREDANT Solutions for HB 1197 Compliance

Data breaches must be publically disclosed – except for properly encrypted mobile devices.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) ensures that security mandates for HB 1197 are consistently and efficiently enforced – regardless of where the data resides.

Only CMG Enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

CMG provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:

- › Ensure that all encryption keys are centrally generated and securely stored automatically on the server before anything is encrypted.
- › Provide confidentiality, privacy and auditing of data residing on any endpoint.
- › Protect sensitive data from unwarranted access, thus reducing risk of internal breaches.

Regulatory overview

Enacted in 2008, HB 1197 requires the Indiana state attorney general to publish notice of a security breach involving personal data managed by companies and requires that the company in question make a comprehensive disclosure of the breach through various media. The bill is published on the attorney general's Internet web site - <http://www.in.gov/legislative/bills/2008/HB/HB1197.1.html>.

The bill defines a security breach broadly as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person." Under the bill, a security breach also includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

The compliance challenge

HB 1197 adds more requirements to a data breach reporting law passed by Indiana in 2006 that only required password protection for mobile devices. This bill requires encryption and other safeguards for data residing on mobile devices. Failure to comply may result in a lawsuit by the Attorney General and an order to pay civil penalties of up to \$150,000.00.

However, companies will not have to report the unauthorized acquisition or pay civil penalties if the device containing personal data meets two conditions. First of all, if all personal information on the device is protected by encryption. Secondly, if the encryption key has not been compromised, disclosed or found to be in the possession of someone without authorization.

Clearly, HB 1197 had added strong incentives for businesses to encrypt all personal data on their customers that is stored on laptops, notebooks, PDAs, smartphones, USB drives and other devices.

CREDANT

More than 700 enterprises and government agencies -- including 50 of the Global 500 – rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.