

# Issue Brief

The Department of Health and Human Services (HHS) has begun posting HIPAA breaches involving more than 500 individuals, as required by s required by section 13402(e)(4) of the HITECH Act. A review of the reported breaches shed light on areas that pose the most risk to organizations as they try to comply with these rules. As of June 2010 the HHS breach website listed 107 breaches. The smallest breach affected 500 individuals while the largest involved more than 1.2 million people.

## **Greatest Risk of a Breach**

One type of breach stands out over all others in terms of total breaches and number of individuals involved. 45 of the 107 reported breaches involve the theft or loss of a laptop computer or portable device containing Protected Health Information (PHI). Another 11 breaches involved a stolen desktop computer. Taken together over half of all reported breaches were the result of the theft or loss of computer hardware containing PHI.

Removable devices have long been identified as a risky area for the loss of PHI. However, the sheer number of these type of breaches is still disturbing, particularly since there is a relatively straight forward solution which significantly limits an organization exposure.

## **Encryption**

The HITECH breach notification rule requires a covered entity to report the breach of “unsecured” PHI. An organization is not required to report a loss of PHI if the data has been secured in a manner approved by HHS. According to HHS regulations PHI “...is rendered unusable, unreadable, or indecipherable to unauthorized individuals if...[it] has been encrypted as specified in the HIPAA Security Rule...”.

To put it simply, if the data on a laptop, portable device, or desktop computer has been properly encrypted it will be considered “secure” and no reporting to individuals or the HHS is required.

## **Summary**

Considering the likelihood of a loss or theft of laptops and portable devices, it is a bit surprising that many organizations have not taken the steps to encrypt data on these machines. While encryption costs money, and takes administrative time and energy to maintain, compared to the risk of major breaches of information it may be a small price to pay. You can access the HHS breach website at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

*While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept liability for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it. This publication is distributed on the understanding that the publisher is not engaged in rendering legal, accounting or other professional advice or services. Readers should always seek professional advice before entering into any commitments.*