Encryption would have stopped many of the patient data breaches caused by lost smartphones, laptops, and tablets, said, Stage 2 Meaningful Use proposal.

In an attempt to eliminate the potential for patient data breaches on mobile devices, the Notice of Proposed Rulemaking (NPRM) for Stage 2 Meaningful Use has proposed that mobile devices, such as laptops, smartphones, and tablets, that retain patient data after a clinical encounter should have default encryption enabled.

Published by the Department of Health and Human Services (HHS) Thursday, the proposed rule for Stage 2 Meaningful Use for the Electronic Health Record (EHR) Incentive Programs noted the increasing number of reported breaches which involve lost or stolen devices.

“We agree that this is an area of security that appears to need specific focus. Recent HHS analysis of reported breaches indicates that almost 40% of large breaches involve lost or stolen devices. Had these devices been encrypted, their data would have been secured,” the NPRM for Stage 2 Meaningful Use states.

The HHS Health IT Policy Committee recommended that health delivery organizations take action to review encryption practices of electronic protected health information as part of their risk analysis.

Dr. Farzad Mostashari, head of the Office of the National Coordinator for Health IT (ONC), further explained the proposal at an ONC town hall meeting Wednesday at the annual Healthcare Information and Management Systems Society (HIMSS) conference and exhibition in Las Vegas.

“There are certification requirements for electronic health records and ... we proposed that there be default encryption of data on end-user devices, unless no data is kept after the session is ended on that end-user device,” Mostashari told the audience.

The proposed measure comes amid several reports that confirm a significant number of patient data breaches have occurred due to the loss or theft of mobile devices. One study from the Ponemon Institute found that the frequency of patient data losses at healthcare organizations increased by 32% in 2011 compared to 2010, with 49% of respondents citing lost or stolen computing devices such as laptops, tablets, and smartphones.

“It has become very clear that one of the major sources of breaches of data comes from lost or stolen devices, and you would not be reading about this loss of data had the information been encrypted,” said Joy Pritts, ONC’s chief privacy officer, during the town hall meeting.

Pritts also said the proposal to encrypt data on mobile devices encapsulates the HIT Policy Committee’s efforts to focus on those areas where “a minimum amount of effort would produce a huge amount of impact.”

Kevin Whelan, Allscripts’ VP of mobility and user experience, said the proposal further shores up data security on mobile devices and notes that “patient data must be encrypted on devices if it’s there, however, patient data is more secure if it is not on mobile devices.”

Continued on page 2
HHS settles HIPAA case with BCBST for $1.5 million

First enforcement action resulting from HITECH Breach Notification Rule 3/13/2012

Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. Leon Rodriguez, Director of the HHS Office for Civil Rights (OCR), announced today. BCBST has also agreed to a corrective action plan to address gaps in its HIPAA compliance program. The enforcement action is the first resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule.

The investigation followed a notice submitted by BCBST to HHS reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the protected health information (PHI) of over one million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR’s investigation indicated BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

“This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program,” said OCR Director Leon Rodriguez. “The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients’ right to private and secure health information.”

In addition to the $1,500,000 settlement, the agreement requires BCBST to review, revise, and maintain its Privacy and Security policies and procedures, to conduct regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA, and to perform monitor reviews to ensure BCBST compliance with the corrective action plan.

HHS Office for Civil Rights enforces the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule gives individuals rights over their protected health information and sets rules and limits on who can look at and receive that health information. The HIPAA Security Rule protects health information in electronic form by requiring entitiescovered by HIPAA to use physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure.

The HITECH Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information, or a “breach,” of 500 individuals or more to HHS and the media. Smaller breaches affecting less than 500 individuals must be reported to the secretary on an annual basis.

Individuals who believe that a covered entity has violated their (or someone else’s) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

Additional information about OCR’s enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

New Malware Threat

A freelance computer consultant in California built virtually undetectable malware. He used various tricks to get people to install this on their computers.

His malware allowed a very personal invasion of their privacy. He read their e-mails, watched them through webcams and listened to them through the microphones on their computers. The information he obtained from his lurking in their computer allowed him to play psychological games with his victims.

The method of distributing his malware was often done by disguising a song on peer-to-peer networks or e-mail, posting it in an instant message to victims disguised as a video.

He is accused of “sexortion” - a new threat where hackers break into your computer and search for compromising photographs that they threaten to post unless some deal is struck.

He is accused of “sexortion” - a new threat where hackers break into your computer and search for compromising photographs that they threaten to post unless some deal is struck.

For a link to the entire article: http://www.computerworld.com/s/article/9219701/

Whelan told InformationWeek Healthcare that Allscripts, which has several thousand physicians using mobile apps to access patient data from its EHRs, has developed a service-oriented architecture that supports its objective of not having data reside on devices. Allscripts’ mobile technology also supports encrypted data queries.

“For the very short time the data resides on the device, there is a secure link back and forth to the device,” Whelan added.

In the meantime, while the risk of patient data loss related to lost or stolen mobile devices has grown, the use of these devices is projected to rise. That trend was evident in the results of the 2012 HIMSS Leadership Survey. One of the questions asked of the 302 health IT professionals was about their top infrastructure priority. Eighteen percent said deploying mobile devices in their healthcare IT enterprise, which was a close second to the 19% of respondents who said their top priority is to deploy servers or virtual servers.

Healthcare providers must collect all sorts of performance data to meet emerging standards. The new Pay For Performance issue of InformationWeek Healthcare delves into the huge task ahead.