LEGACY
HEALTH

Frequently Asked Questions RE: The HITECH Act's Breach Guidelines

Q: What is HITECH?

A: The Health Information Technology for Economic and Clinical Health (HITECH) Act was set in motion in 2009 as part of the American Recovery and Reinvestment Act. It provides the healthcare industry over $31 billion in stimulus funds dedicated to infrastructure improvements, including the adoption of Electronic Health Records (EHR). The HITECH Act includes a number of measures designed to broaden the scope and increase the rigor of HIPAA compliance. HITECH contains new privacy and security requirements for Protected Health Information (PHI), including data breach notification and penalties for non-compliance.

Q: How is HITECH different from HIPAA?

A: Under HIPAA, breach of privacy or security of PHI did not require patient notification by a healthcare provider or Business Associate. The HITECH Act mandates patient notification in most circumstances. Under HITECH, an organization that has a data breach is required to notify each individual affected by the breach. This new notification requirement applies to all entities that hold PHI, including Legacy's Business Associates.

HITECH also requires organizations to report data breaches to the Department of Health and Human Services (DHHS). This publicly available report will account for every breach which occurred during the previous year, including mis-directed faxes and mail.

Q: What is a breach?

A: A breach is any unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information. A breach may involve PHI in any form, paper or electronic. "Compromises the security and privacy" of PHI means "poses a significant risk of financial, reputational, or other harm to the individual." Any exceptions to this definition will be determined through the investigation and response process.

Q: How do I report a breach?

A: Report a breach by calling the HIPAA Hotline, at **503.413.4495**. If you are unable to call the hotline, you may also report through Legacy's secure website: www.MyComplianceReport.com.

It is important to report a breach as soon as you are aware of it. Legacy will need to take steps to investigate the breach and protect our patients' information as quickly as possible.

Q: What details do I share when reporting a breach?

A: The more information you provide when reporting a breach, the quicker the investigation and response team will be able to act. Please provide the HIPAA Hotline with your name and contact information; the time and location of the breach; when you found out about the breach; and a description of the incident, with any supporting

details you can provide. You may make an anonymous report by withholding your contact information but that may impede the progress of the investigation and response.

Q: What if I am not sure if an event is a breach?

A: Report it using the HIPAA Hotline, **503.413.4495** or www.MyComplianceReport.com. Data breach reporting is required by law and Legacy policy. If you are uncertain if an event constitutes a breach, report it. The investigation and response team will determine if a breach occurred.

Q: How will this affect my day-to-day operations?

A: The new HITECH regulations should not affect your daily job routine. The only update is making sure you report any potential breaches to the HIPAA Hotline, **503.413.4495** or www.MyComplianceReport.com as soon as possible. The investigation and response team will determine if patient notification is required.

Q: What happens if I do not comply with HITECH?

A: The legislation increases civil and criminal penalties for Privacy Rule violations. Fines for security breaches start at $100 and can go as high as $1.5 million. Legacy will take appropriate corrective actions in the event an employee violates Legacy policy or the law. Appropriate corrective action is determined based on the situation but will include disciplinary action up to and including termination of employment.

Q: What are some examples of breaches?

A: Specific examples of breaches are:

- A hospital billing department sends a bill to the wrong individual which is opened by the recipient.
- Lost or stolen laptops or PDA
- Loosing a medical record
- An employee snooping in a patient's file
- A clinic mails lab results to the wrong patient.
- A hospital employee who is not authorized to access protected health information decides to look through patient files in order to learn of a friend's treatment.
- A briefcase containing patient charts is stolen from a health care provider's car
- A hospital employee accidentally gives a discharge order form to the wrong patient.
- A reminder notice for an appointment at an infectious disease physician's office is mailed to the wrong address.