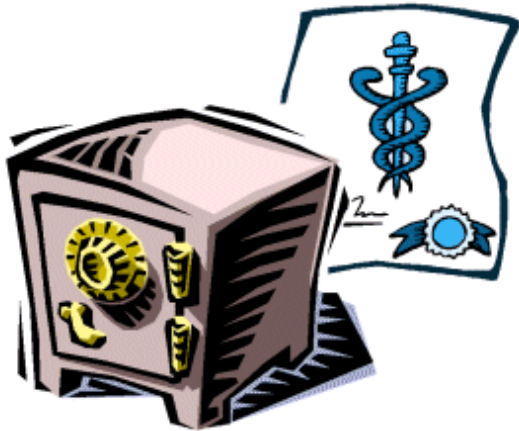


HIPAA Security for Healthcare Staff



Web-Based Information Security Training from Cosaint



The course discusses:

- What is a virus and how might it affect you?
- How can you get a virus?
- How to handle e-mail attachments
- What to do if you think you've been infected
- Hoaxes and chain letters
- How to handle passwords safely
- How to choose good passwords
- Monitoring of login success/failure
- The importance of Physical Security
- Danger Signs indicating Social Engineering
- Risks inherent in unsecured e-mail

The final version of the HIPAA Security Rule was issued by the DHHS in February, 2003 and covered entities such as health plans, hospitals and clinics must comply with the rule by April 21, 2005.*

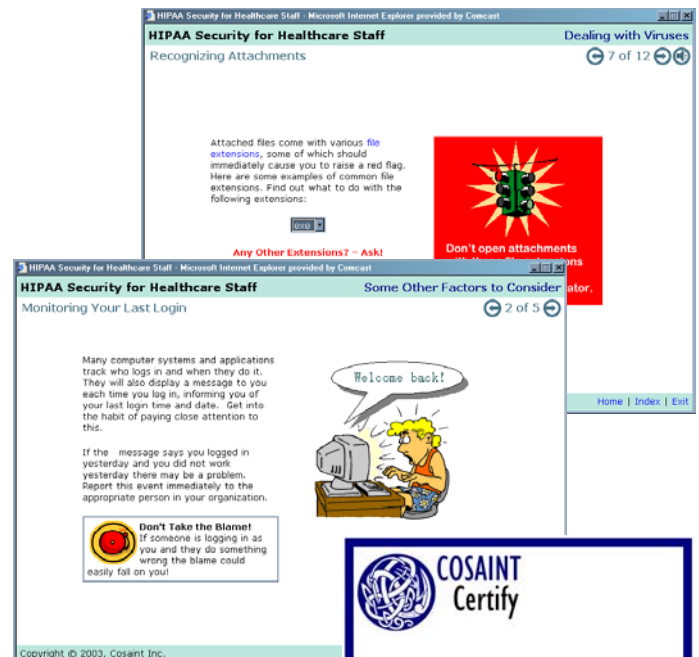
The Security Rule covers a wide range of provisions to improve the way that patient information is secured against disclosure, modification or destruction. It also requires that all staff (including management) with access to patient information must be provided with security awareness training including specific topics such as avoiding malicious software, managing passwords and monitoring login success/failure.

This course covers these key elements and also touches on Physical Security, Social Engineering and security of E-Mail messages.

The course includes interactive exercises, an optional audio track, and a short mastery test to verify that student has understood the material. On successful completion of the test, the student is issued with a certificate with a unique authentication code.

Because of the breadth of the HIPAA Security Rule, this course takes approximately 60 minutes to complete.

* Small health plans may have until April 21, 2006.



www.cosaint.net