

## Virus Policy Dept. of Surgery

### Background

#### Revised HIPAA Regulations

- Enacted by the American Recovery and Reinvestment Act of 2009 (aka the Stimulus Package), Title XIII: Health Information Technology for Economic and Clinical Health (HITECH), signed into law by President Obama on 2/17/2009
- Most provisions take effect on 2/17/2010; however, increased penalty provisions were effective immediately
- Breach is defined as “unauthorized acquisition, access, use or disclosure of protected health information.”
- Notifications in the case of breach:
  - We must notify each individual whose PHI has been compromised.
  - We must report breach to the Secretary of the Dept. of Health and Human Services, who will post to the HHS public web site the names of all institutions involved in breaches of over 500 individuals.
  - If breach involves more than 500 NC residents, we must notify prominent media outlets.
- New penalties
  - Tier A: offender did not know, and by exercising reasonable diligence would not have known, that he/she violated the law - \$100 per violation, not to exceed \$25,000 in a calendar year
  - Tier B: violation was due to reasonable cause and not willful neglect - \$1000 per violation, not to exceed \$100,000 in a calendar year
  - Tier C: violation was due to willful neglect but was corrected - \$10,000 per violation, not to exceed \$250,000 in a calendar year
  - Tier D: violation was due to willful neglect and was not corrected - \$50,000 per violation, not to exceed \$1,500,000 in a calendar year
- By April 17, 2009, the Secretary of Health and Human Services is to issue guidance “specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.”
- Full text of the American Recovery and Reinvestment Act of 2009 is available at [http://www.whitehouse.gov/the\\_press\\_office/arra\\_public\\_review/](http://www.whitehouse.gov/the_press_office/arra_public_review/) (see page 146 for Improved Privacy and Security Provisions)

### Policy – IT Response

#### Upon report of virus:

- Request that user detach network cable and refrain from using computer
- Record virus name and/or behavior
- Remove hard drive from computer
- Ask user to complete Sensitive Information Report and Local Data List
- Set hard drive aside for minimum of one hour – to determine how wide-spread virus might be

#### If computer does not contain PHI, or

#### If computer contains PHI but virus research reveals insignificant threat:

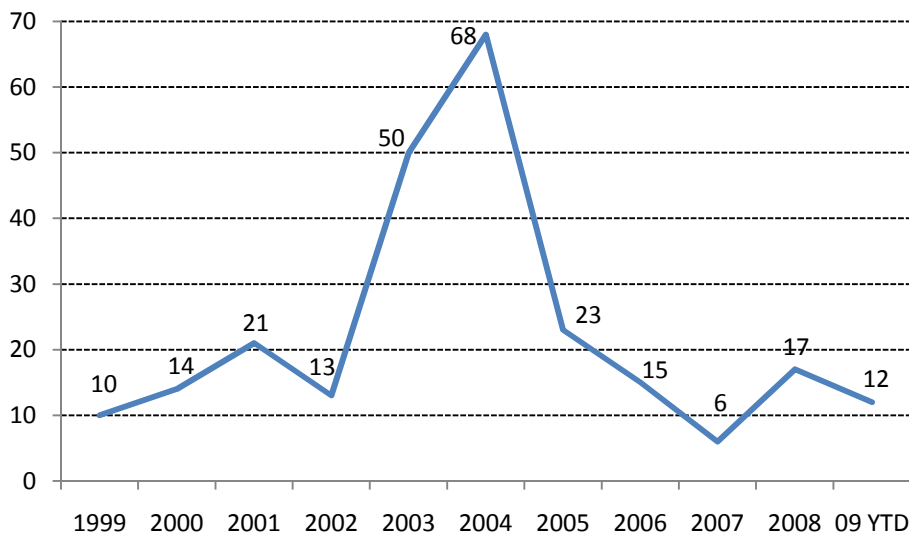
- Perform Symantec/Malwarebytes/SuperAntiSpyware scans on hard drive – connected as slave
- Once identified, research virus to find, and then follow, removal instructions
- When all scans are clean, return hard drive to user computer, and repeat scans
- Force Surgery domain password change
- User must complete HIPAA training module 2, General Information Security

If computer contains PHI:

- Locate/purchase replacement hard drive
- Copy local data from infected hard drive to repository (isolated from network)
- Rebuild image on new hard drive
- Copy local data onto new hard drive
- Scan local data and disinfect if necessary (i.e., following steps identified above)
- Install replacement hard drive in user computer, and repeat scans
- Force Surgery domain password change
- User must complete HIPAA training module 2, General Information Security
- Submit original hard drive to OIS for forensics

Note: Per OIS, PHI on an infected computer is considered compromised if forensic evidence fails to demonstrate that sensitive information was NOT accessed, acquired or disclosed.

### Virus History in Dept. of Surgery



Per OIS, Symantec detects only 27% of viruses.

### Recommendations

- Do not open e-mail attachments that are not expected or from someone you don't know (e.g., "A Friend")
- Do not open ANY attachments sent to your personal e-mail account (e.g., gmail, yahoo, roadrunner, etc.)
- Do not install, download or use non-essential software: Instant Messenger, AOL, iTunes, weather updates, coupon clipper, games, sporting events, etc.
- Avoid frivolous web sites: eBay, FaceBook, electronic greeting cards, electronic event planners
- Don't use work e-mail accounts for non-work-related activities
- Budget for replacement hard drives (~\$60 each)
- Minimize PHI information, especially that stored on the local hard drive (including local mail folders)
- Work off mapped drives – will minimize downtime associated with virus infection



