Information for BOCC re HIPAA Process

I. Steps in HIPAA Breach Identification and Notification

A. Investigate

B. Determine if PHI compromised

If yes,

C. Mitigate Immediate Harm

D. Develop Remediation Plan

1. Changes to policies and procedures
2. Training
3. Sanctioning workforce members

E. Breach Notification

II. HIPAA Breach Notification

A. Timing – without unreasonable delay but no later than 60 days following discovery

B. Content –

1. Description of what happened, date of breach and date of discovery
2. Description of health information disclosed
3. Steps people should take to protect themselves from harm
4. Description on investigation and mitigation
5. Contact information for individuals to ask questions

C. Method –

1. Individual notice – letter to individual
    a. Substitute notice, via media or website, if unable to contract 10 or more individuals
2. Media notice – if breach affects 500 or more individuals
    a. In addition to individual notice
    b. Press release to prominent media outlets
3. Secretary of DHHS
    a. Within 60 days if 500 or more individuals affected
    b. Within 60 days of end of calendar year if less than 500 individuals affected
    c. Completion of Electronic Breach Report form on HHS website

Potential HIPAA fines:

Various categories of fines:

Category 1: minimum fine of 100 per violation up to 50K

Category 2: minimum fine of $1000.00 per violation up to 50K

Category 3: minimum fine of $10,000 per violation up to 50K

Category 4: minimum fine of $50,000 per violation.

The max fine per violation category per year is 1.5 million

Current Public Information Process

- Public Information Request comes in and is received by Public Information Department and forwarded to County Attorney for approval to proceed pulling the requested information
- The County Attorney forwards the Pubic Information request to Information Security via email to begin pulling the requested emails
- IT security provides the County Attorney with the requested emails
- The County Attorney manually goes through the selected emails
- IT Security confirms that the deleted items to be redacted are removed
- Once the County Attorney is finished with the review, IT Security burns the CD for the requesting party

Stop-Gap Measures

- IT Security captures the total number of emails retrieved for the request
- County Attorney continues to review the initial file
- The Senior Associate Attorney makes a second pass at the selected emails
- IT Security compares the original total number of emails retrieved to that which was returned from the attorneys
- The IT Security Department Supervisor ensures that the "Deleted Items" folder is cleaned out and information is burned to a disk
- The County Attorney makes a final pass of information before it is released to the requestor

Long-Term Process

Over the next few weeks we will

- Outline potential "future state" process considerations
- Review with executive sponsor and establish an executive level charter defining the why, the what, the how and the when. This will clarify scope and resources needed to advise the Executive Team of the resources needed to establish a project.
- Align resources required to initiative a deliver solution defined in the executive charter