ADDITIONAL PROTECTION REQUIREMENTS UNDER CMG CYBER LIABILITY PROGRAM

Catholic Mutual has partnered with Tokio Marine HCC to provide Cyber Liability coverage to all our members with a $250,000 limit. However, quotes can be obtained for additional limits up to $10 million. To help enhance your ability to obtain higher limits, your (Arch) Diocese should implement the following policies/procedures:

- Secured configured firewall protection throughout your (Arch) Diocese. See enclosed:
    - Sample Data Security Policy

- Anti-virus software updated on a monthly basis on all desktops, portable devices and mission critical servers. See enclosed:
    - Sample Protection against Malicious Programs Policy

- Privacy and security policies in place that addresses mandatory training that is followed by employees, contractors and other individuals with access to private medical or financial information. See enclosed:
    - Sample Information Security Policy
    - Organization Acceptable Use Policy

- All stored personal and/or confidential data on portable devices, including laptops, PDAs, back-up tapes, USB thumb drivers and external hard drives must be encrypted to industry standards. See enclosed:
    - Sample Removable Media Policy

- HIPAA program must be in place for any organization required to follow HIPAA compliance. See enclosed:
    - Information Access Management Policy

In addition, the following security needs to be in place in order to be considered for the PCI – DSS Assessment Coverage Endorsement (Coverage for fines and penalties levied by the Payment Card Industry Data Security Standards against merchants due to PCI DSS non- compliance) and Cyber Crime Coverage Endorsement (financial fraud, telecommunications fraud and phishing attacks):

- All processing, storing, transmitting or handling of credit or debit card data must have data security controls that are compliant with the Payment Card Industry Data Security Standards. See enclosed:
    - Sample Payment Card Information Security Policy

- Wire transfer protocols must prohibit one employee from controlling a transaction from beginning to end.

For additional information, please see the Cyber Liability Risk Management section on your Member Home page.


TOKIO MARINE
HCC