

DRAFT - ABSTRACT



CYBERWAR WORKGROUP

© 2005 The Medical Banking Project. All Rights Reserved.

Workgroup Members:

Robert Thompkins-Bey, President & CEO, Bey Technologies International, Inc.
John Casillas, Chair of the Medical Banking Institute, Executive Director of the Medical Banking Project

Sponsor/Organizer:



320 Main Street, Suite 230
Franklin, TN 37064
www.mbproject.org

Third National Medical Banking Institute

Educational Grantor:



DRAFT

Statement of Purpose

The MEDICAL BANKING CYBERWAR WORK GROUP is an independent, vendor-neutral, collaborative forum that is seeking to define relevant issues and address potential best practices models that respond to risk areas in medical payment channels. The Work Group will examine medical payments infrastructure, new IT technologies, business processes and other areas that relate to risk mitigation in times of crisis.

DRAFT

Abstract

Why are medical payments important to homeland security? The answer may not be so obvious and frankly, the same issue caught the entire banking industry off-guard as regards HIPAA¹. Institutional medical payments contain individually identifiable health information in the form of an explanation of medical benefits ('EOB'). For a provider, EOB information is critical because it shows what procedures the health plan reimbursed partially, fully or not at all. Thus the EOB is a detailed medical record and accordingly, medical payment channels are fraught with the same privacy and security risks as other aspects of healthcare operations.

When medical payments contain sensitive personal health information what national risks or vulnerabilities could emerge? We are entering unknown territory and need more time to devote to this uncomfortable topic. The areas under review include:

The impact of revised UCC Article 9, proposed Bankruptcy Reform Act and the UNICITRAL Convention on cross-border transfer of receivables (containing PHI); Anthrax contamination of a lockbox and the impact on hospital cash flows; fraudulent financial transfers to enemies posing as physicians in Medicare system; using asset-backed securitizations to acquire sensitive health data; wireless communications; black mail, custom biological warfare, (high profile individuals); impacting public confidence in our healthcare system via PHI from payment channels that is routinely disclosed in public places.

¹ See MBProject's White Paper written in 1998; it suggests that HIPAA impacted banking services for medical providers, but was largely ignored by the banking community until our first HIPAA Policy Roundtable where HHS unofficially confirmed our findings.

DRAFT

Workgroup Recommendations / Observations

- Track all sales of medical receivables, whether via securitization or otherwise; track all healthcare bankruptcies and the affected lenders, as this could result in a transfer of PHI.
- Create center of excellence for studying potential threats to critical infrastructure with emphasis on unique structures that support medical payments and remittances (i.e., lockbox, new payor-side processors).
- Link sanctions data-base of Medicare providers with other intelligence to isolate potential payments to fund terrorist activities.
- Link OFAC database with charity workers database to determine any fraudulent funds transfers through charity fronts.
- Create suggestions for infrastructure improvements in medical payment channels using risk grid.