

501-225-3653 P
501-221-9068 F
6301 RANCH DRIVE
LITTLE ROCK, AR 72223
WWW.ACMINET.COM



Transforming Care Management Through Innovation

DATA PRIVACY AND SECURITY ANALYSIS

A review of INTERMED Integrated Health Behavioral Assessment Tool

Michael Terpening, Integrity Group, CMI
April 30, 2009

Table of Contents

Overview.....	2
Intermed Application Review.....	3
HIPAA Overview.....	4
HIPAA Implication of Intermed Application.....	4

Overview

CMI is partnering with INTERMED, a company in the Netherlands, to provide access for Case Managers to a web based Integrated Health Behavioral Assessment Tool. The access may be granted to health plans, other health care entities, and individual case managers. The database for the application is to be hosted in the U.S. where the web server would also reside. However, administration of the system may occur from off-shore.

A demonstration of the application and review of system and data procedures and plans took place on Friday April 24th in a web conference attended by the creator, Dr. Frits Huyse, his key IT leader, Jeroen Bos, and the CMI team lead including the CIO, Ted Howard, the Executive Director Cheri Lattimer, and a CMI/Integrity consultant Michael Terpening.

Assessment of the data security in light of HIPAA privacy act legislation was goal of the application review

This analysis:

- Outlines the high level architecture of the application service
- Lists the existing privacy protections
- Notes implications for the application based upon the U.S. HIPAA privacy act
- Provides some suggestions for enhancement in data storage, transfer, security, or access permissions.

This analysis concludes that the existing data security in the Intermed system is adequate to support HIPAA compliance as it was presented in the demonstration.

Intermed Application Review

Key features of the Architecture

- Web based – ASP hosted on a separate server from workstation
- Data may be hosted separately from server or combined (as planned in Little Rock)
- Display GUI using AJAX on workstation over 256bit SSL encryption for data
- XML message based export data with encryption for external applications (health plans systems)
 - Current HL7 compatible (version 2) an XML HL7 version 3 enhancement possible in the fall of 2009 that could encrypt
- Data will be hosted in U.S. (Little Rock) system/application maintenance may take place from overseas.
- Internationalization done at the application label and drop down values using a highly configurable spreadsheet approach for multiple language support. (Note that with all internationalization, only labels and values can be translated, not textual data)

Key aspects of Administration

- Multiple levels of security:
 - Intermed administrator (highest level) can create organizations and see/maintain all organization data
 - Organization administrator can create users but cannot see other organizations users or data
 - Users (lowest level) are associated with an organization but cannot see other organization data or other users data
 - Users currently enter in all Patient related demographic information and thus 'own it'. There is no patient data upload capability.
 - Groups of users with like permissions will be possible in the June 2009 release
 - An audit trail is possible for all button pushes performed in the application by each lowest level user

Key features of patient information

- Entry of demographic information for each patient assessed
- Patient identifiers can be encrypted in the database and decrypted on the web display
- Reports and Letters with PHI may be created as part of user workflow and printed, faxed, or saved on local workstation drives.
 - Reports may show multiple patient assessment results on same report
- New version will allow a link to a patient to completed an assessment questionnaire

Key security constraints

- Encryption of data at 256kb exceeds 128kb recommendations for secure sites
- Administrator can limit IP addresses for XML data transfers to trusted sites

HIPAA Overview

HIPAA privacy protection legislation is aimed at securing patient information from disclosure to anyone not directly involved in the treatment of that patient. It is specifically designed to address electronic records though it also covers the disclosure of printed materials.

HIPAA constraints are applied to 'covered entities' which may be health care providers (including Case Managers), Health Plans and Health Care Information Clearinghouses. There are no direct provisions related to offshore data storage of Patient Health Information (PHI). Individual citizens of the United States cannot sue based on HIPAA, rather HIPAA is enforced by the Health and Human Services department of the federal government.

States within the U.S. may add more stringent controls to the HIPAA privacy act. Some states have done so requiring written consent before sharing information between covered entities and many states have applied these written consent requirements to mental health information disclosures as well.

HIPAA Implications for the Intermed Application

Intermed as a decision support application suite and data repository may not be a 'covered entity' itself. The Intermed system is not a health plan, however will potentially be used as a business partner via CMI with health plans who may require HIPAA transactions. Intermed is likely not an information clearinghouse but as Microsoft and Google Health, who both claimed not to need HIPAA compliance, have recently learned, even a Patient Health Record may require a variation of HIPAA umbrella protection.

In February of 2009, the Federal Trade Commission proposed a provisional rule that would cover these borderline situations. The proposed FTC interim rule also would apply to PHR-related entities, including those not covered under the privacy and security provisions of HIPAA, specifically, those: "that offer products or services through the website of a vendor of personal health records, that are not covered entities (as defined by HIPAA) and that offer products or services through the websites of covered entities that offer individuals personal health records," and "that are not covered entities and that access information in a personal health record or send information to a personal health record".

Taking the provisional rule into consideration, it may be prudent for Intermed to attempt to comply with all HIPAA regulations.

Analysis of the existing data protection does not expose any obvious weakness in the Intermed security to be HIPAA compliant, however a few points may be considered to improve that security in consideration of any more stringent State by State rules or business partner needs for accreditation by NCQA, National Committee for Quality Assurance, a body that certifies health plan care management programs.

Application Analysis and Recommendations

1. Intermed is planning to store patient data in a server in the U.S. which must include adequate permissions for users. The multi-level role based security in place currently should provide administrative protections. There are a few potential issues.
 - a. The highest level security has access to individual detail database contents during troubleshooting and data repairs. This is common with the vast majority of system vendors of Health Care related applications. To address this issue in good faith the following should be considered
 - i. **Patient identifiable information including names, social security numbers and even age, gender and address should be encrypted in the data server if possible. The encryption key could exist on the client workstations so that data passing across the internet is encrypted.**
 - ii. **Clear policy and procedures for the protection and non-disclosure of PHI should be written and followed at the data center for highest level role.**
 - b. All levels of role based security should have an audit trail in the application itself. Current functionality covers a record of 'button pushes' or user actions, however it does not cover specific patient record viewing or report fax/printing contents.
 - i. **Many systems have audit trail records that track the results of SQL searches down to the individual patient so they store the date/time of each user accessing each patient record. (NCQA)**
 - c. **Some health care information Health Risk Assessment vendors provide security by keeping the PHI information local to the user workstation and passing non-PHI data through a 'black box' to arrive at health risk scores. This is less useful when longitudinal records need to be kept and compared over time.**
 - d. **If data is ever to be stored off shore of the U.S. Some states, in the near future, may require a patient consent for that PHI.**

2. Intermed plans to provide a user with a disclaimer to outline their responsibilities in securing the privacy of health information and patient identities.
 - a. **The proposed disclaimer should require a mouse click to 'accept' – this is acceptable at login and does not need to be performed for each patient record creation. However, some health care information systems do present it at each patient record initiation.**
 - b. **Warnings could be provided whenever faxing any report with PHI included that the recipient fax machine must be secure and not available to unauthorized individuals.**
 - c. **Disclaimer may include mention that patient reports saved locally on the workstation drives are still subject to non-disclosure rules.**

3. Intermed data is likely to be shared with business partners. These are HIPAA covered entities such as health plans, case manager groups, and individual case managers. It is likely that the Health Plans will want to receive data transactions in some format with the results of the assessment and the inclusion of PHI identifiers. Covered entities that already used HIPAA transaction sets will require that Intermed also use those transactions.

If the entity does not use HIPAA sets a secure transfer of data is still required. This can be handled in a number of secure ways:

 - a. **The proposed XML HL7 message (version 3) enables encryption and decryption at both ends. Intermed proposes to support this standard, however, it would require that the health plan already be capable of supporting the standard as well.**

- b. The patient identifiers could be stripped from messages or masked/encrypted for decryption by the health plan data store and only the HRA scoring sent to the partner entity. (see black box model, 1c).**
- 4. Intermed has plans to enable individual patients to complete an assessment on line and record results separately from the health provider created assessment record. This was to be done by providing a link in an email to a patient directing them to the assessment site.
 - a. If the patient is to be given a view of the assessment over time, they should be provided with a password protected access. This is typically provided by secure site entry by the patient of key personal information which is used to verify identity, and send a temporary password to an email account. The user then logs into the assessment site and changes password immediately.**
 - b. No PHI data should pass via regular email to or from the provider or patient, or the patient and the site. This can be controlled by creating a secure email-like communication tool within the assessment site itself that may notify the other party that a secure message awaits at the site. The notified party would then log into the secure site to view and reply.**