



**Integrated Management Solutions**

## COTTS HIPAA Compliance Statement

To the best of our knowledge we followed all guidelines in complying with HIPAA security and privacy regulations in development and the deployment approach for our Court Ordered Treatment Tracking System (COTTS) product. We believe process controls are in place within COTTS to permit the customer to comply with HIPAA in the use of COTTS. Further we believe the deployment approach using firewalls and the developed security module are sufficient to meet HIPAA security issues. Many of the HIPAA regulations relate to administrative and operational procedures, we believe COTTS meets those requirements. This statement highlights development and deployment aspects of COTTS to provide confidence that requisite privacy and security standards are met. The elements of HIPAA most pertinent to Drug and Community Courts are discussed below with annotation of iMs and COTTS compliance.

Security—relates to the means (process and technology) by which an entity protects the confidentiality of health information. The goals of security measures are to keep information secured, and decrease the means of tampering, destruction, or inappropriate access. There are four categories of requirements:

- Administrative Procedures—documented, formal practices to protect data
  - While the majority of administrative procedures are under the control of the entity, COTTS was designed to permit the implementation of procedures to ensure protection of data.
- Physical Safeguards—protect data from fire, other natural and environmental hazards, and intrusion
  - User COTTS hosting will require appropriate physical safeguards.
  - iMs hosted deployment recommendation provides a secure/locked location at an ISP with 24 hours surveillance and appropriate protections from disaster.
- Technical Security Services—protect information and control individual access to information
  - Password protections determined by system and/or vendor administrators restrict access to database information.
- Technical Security Mechanisms—guard against unauthorized access to data over communications network
  - All data transmissions are protected with industry standard 128-bit encryption.

Privacy—refers to the individual's right to keep certain information private, unless that information will be used or disclosed with his or her permission. Privacy topics include:

- Consent/Authorization Issues/Procedures/Processes
  - Appropriately designated individuals and formal procedures within COTTS determine control of access.
- Business Associates Requirements

iMs has a history and in place Business Associate Agreements related to HIPAA and other security and privacy issues. Our parent is a DoD Top Secret cleared organization so we have extensive experience with maintaining security and it is a high priority for all our business. iMs and specific employees will sign Business Associate Agreements as required.