Proposal to Healthcare Providers

on how to adhere to

Regulatory Requirements, and insure a Safe Workplace

(Related to "Patient Protection and Affordable Care Act" – PPACA)

including:

- **HIPAA, HITECH, ePHI, and the Final Ombudsman Rule (Medicare / Medicaid)**
- **Workplace Safety, Security and Threat Elimination Via Workplace Violence Prevention (OSHA, DHS, NFPA 1600 and OEM), and mandated**
- **Workflow Optimization / Employee Training Management.**

Proposed by:

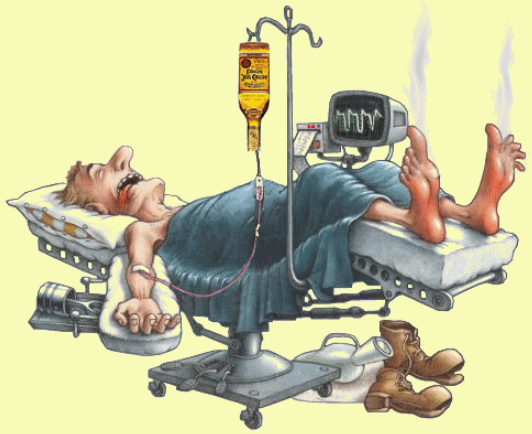
Thomas Bronack, President
Data Center Assistance Group, Inc.
15180 20th Avenue
Whitestone, New York 11357
Email: bronackt@dcag.com
Cell Phone: (917) 673-6992

Audience Includes:

- Hospitals, Clinics, Doctors Offices; and
- Business Associates providing services to Healthcare Organizations.

Healthcare is Sick and Needs to be Fixed (Medicare / Medicaid)

- **Patient Costs Soar, while Services Suffer:**
  - Redundant Testing and Litigation Fears;
  - Inefficient workflow and supply chain operations;
  - New Patient Freedoms allow for the Sharing of Patient Authorized Medical Records, while restricting unauthorized use and sale of data;
  - Improved Electronic Collaboration for remote assistance;
  - Examining Medical Information to uncover trends , diagnose symptoms, and formulate remediation's.



- **Laws and Regulations must be adhered to, including:**
  - **HIPAA** – Health Insurance Portability and Accountability Act (1996) to improve awareness and efficiency;
  - **HITECH** - Health Information Technology for Economic and Clinical Health (2009) includes more stringent regulations and sanctions;
  - **ePHI** – electronic Personal Health Information (2009) to safeguard all forms of patient information (paper, electronic, video, audio, etc.) against unauthorized use and sale;
  - **Final Omnibus Rule** (1/25/2013) states specific compliance guidelines and defines the final Privacy, Security, and enforcement fines and sanctions:
  - "**Meaningful Use**" clause can reimburse electronic record conversion ($40-60K);
  - **Patient Protection and Affordable Care Act** (PPACA), sometimes known as Obama Care;
  - Healthcare Organizations and their Business Associates **must comply by 9/23/2013**;
  - **States Attorney Generals** can bring lawsuits on behalf of private individuals for breach of Privacy Rules; and,
  - Compliance will be **aggressively enforced** to reduce cost and improve patient services.
- **Applies to** Healthcare Organizations and their Business Associates.
- **Designed to** improve services and reduce costs through new technologies and procedures.

Purpose of Presentation and Deliverables that can be achieved

- Define **healthcare industry** **New and Existing Compliance Regulations**;
- Review **Patient Protection and Affordable Care Act** (referred to as - Obama Care);
- Discuss **New Patient Freedoms** related to **patient information sharing**;
- Show how "**Joint Commission Accrediting Healthcare Organization**" (**JCAHO**) **certification** can be achieved and why it is a benefit;
- Suggest **methods** to perform Risk Management, Auditing, and Incident Reporting;
- Demonstrate how **better utilization of Information Technology**, Data Management, and Access Controls can create a safeguarded and efficient environment;
- Determine **Security and Emergency Response** Planning needed to "***Protect the Workplace***", "***Safeguard Patients Rights***", and "***Comply with Regulatory Requirements***";
- Create a project plan / road map to Implement **Physical and Data Security**;
- Assist in the development and Implementation of **Emergency Response Plans**;
- Implement a **Workflow Management System** to insure Forms Management and Controls;
- Document new **Standards and Procedures** needed to better protect patients, achieve a safeguarded environment, and improve efficiency;
- Provide **Employee Awareness and Training**; and,
- Provide **Integration, Support, and Maintenance** going forward.

Audience and Compliance Requirements

Healthcare Industry	• Hospitals; Clinics; Doctors Offices; and, • Business Associates and Sub-Contractors.
Patient Security & Safety	• HIPAA; HITECH; ePHI; and Final Omnibus Rule. • "Meaningful Use" reimbursement for electronic data ($40-60K)
New Patient Freedoms	• Ability to have records transferred by request of patient or their authorized representative (Record Sharing).
Workplace Protection	• Responsible for protecting employees, patients, and visitors; • OSHA, DHS, OEM, and NFPA 1600; • Workplace Violence Prevention; • Workplace Physical Security and Evidence Capturing; and, • Ability to evacuate patients in Emergency Mode.
Penalties and Financial Losses	• Criminal and Civil penalties; fines up to $1.5 million per occurrence taking effect 9/23/2013.
Training and Awareness	• Staff must be aware of requirements and trained on how to respond to a wide-range of disaster events.
Risk Management	• Identification of Risks and potential Disaster Event obstacles.
Response Identification and Planning	• Mitigate Gaps and Exceptions; Mediate obstacles blocking the ability to respond to Disaster events; insure the ability to respond to encountered incidents; have the ability to provide a safeguarded environment capable of providing enhanced protections and efficiency while achieving compliance. Integrate within the everyday functions and environment.

Who is effected by these changes?

Business Associates and Contractors including:

- Physical (Guards, CCTV, Card Keys, etc.) and Data Security Service Providers;
- IT Equipment, Software, Consulting, and Support Vendors;
- Lawyers, Accountants, and Auditors;
- Leasing firms and other financial providers;
- Telephone and Communications Vendors;
- Shredding Vendors, Waste Disposal, and Transportation;
- Primary and Secondary Data Centers;
- Cloud Computing and Virtualization Service Providers;
- Answering Services for Medical Offices;
- Medical Billing Services;
- Medical Transcriptions Services;
- Medical Collection Agencies; and,
- Cleaning, Disposal, and internal Service staff.

The best protection is to perform a Risk Analysis to determine regulatory gaps and exceptions that must be mitigated, along with impeding obstacles that must be mediated. Then implement controls and procedures to create a safeguarded and compliant environment.

History and purpose of HIPAA rules and regulations, from original to current updates.

- **1996** - Initially **HIPAA** was introduced to improve efficiency and effectiveness of the U.S. Healthcare System through guidelines and regulatory requirements.
- **2/2009** – (**HITECH**) Health Information Technology for Economic and Clinical Health Act was introduced as part of the **American Recovery and Reinvestment Act** covering health records from paper based through all types of current and future electronic health records.
- **1/25/2013** – The **Final Omnibus Rule** was published by the **Federal Register** to include **more stringent privacy and security protection for patients** **(to be en-acted 9/23/13)**.
  - Rule also increased **sanctions and penalties** for failure to comply, including the right of States Attorneys General to bring lawsuits on behalf of private individuals for breach of the Privacy Rule.
  - The Security Rule expands data protection to include electronic media and electronic Personal Health Information (**ePHI**) - **covering paper, video, OCR, Social Media, and electronic media**.
  - Although HITECH has been enforceable since **2/2010** many organizations have failed to take action to fully comply, thereby risking **penalties, financial loss, patient services, and reputational loss** that could damage the ability to continue serving the public's medical needs.
  - Included in **Patient Protection and Affordable Care Act** (Obama Care) to reduce costs and improve service.
- **HIPAA** was developed to improve the education of hospital and medical record keepers on the rules and regulations that must be followed to safeguard patients. The **Final Omnibus Rule** and **Patient Protection and Affordable Care Act** provide a more detailed explanation of these safeguards and how best to protect the rights and privacy of patients.

HIPAA Contingency Planning and Security Guidelines (newly updated)

Administrative Safeguards include:

- **Security Management Process** (for People, Physical Environments and Data);
- **Assigned Security Responsibility** (Management through all levels of Personnel);
- **Workforce Security** (Procedures governing personnel Screening through Termination);
- **Information Access Management** (Data Sensitivity, Access Controls, Backup / Recovery, etc.)
- **Security Awareness and Training;**
- **Security Incident Procedures** (from identification through "Root Cause" analysis, resolution; Logging, Tracking, Reporting, and Repository Maintenance);
- **Contingency Plan** (Disaster, Business, Emergency, and Crisis Management Responses);
- **Evaluation** (Risk Analysis and Periodic Reviews, with Attestation by Executive Management); and,
- **Business Associate Contact and Other Arrangements** (from definition to accreditation).

Physical Safeguards include:

- **Facility Access Controls (Physical Security to produce a safe workplace);**
- **Workstation Use;**
- **Workstation Security; and,**
- **Device and Media Controls.**

Technical Safeguards include:

- **Access Controls (Data Security and elimination of Data Corruption);**
- **Audit Controls;**
- **Integrity;**
- **Person and Entity Authentications (User Entitlements); and,**
- **Transmission Security (Local and Remote / Encryption).**

Penalties for non-Compliance

CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation Category Section 1176 (a) (1):	Each Violation:	All such Violations of an identical provision in a calendar year:
A. Did Not Know	$100 to Max of $5,000	$1,500,000
B. Reasonable Cause	$1,000 to Max of $50,000	$1,500,000
C. 1. – Willful Neglect – Corrected	$10,000 to Max of $50,000	$1,500,000
C. 2. – Willful Neglect – Not Corrected	$50,000	$1,500,000

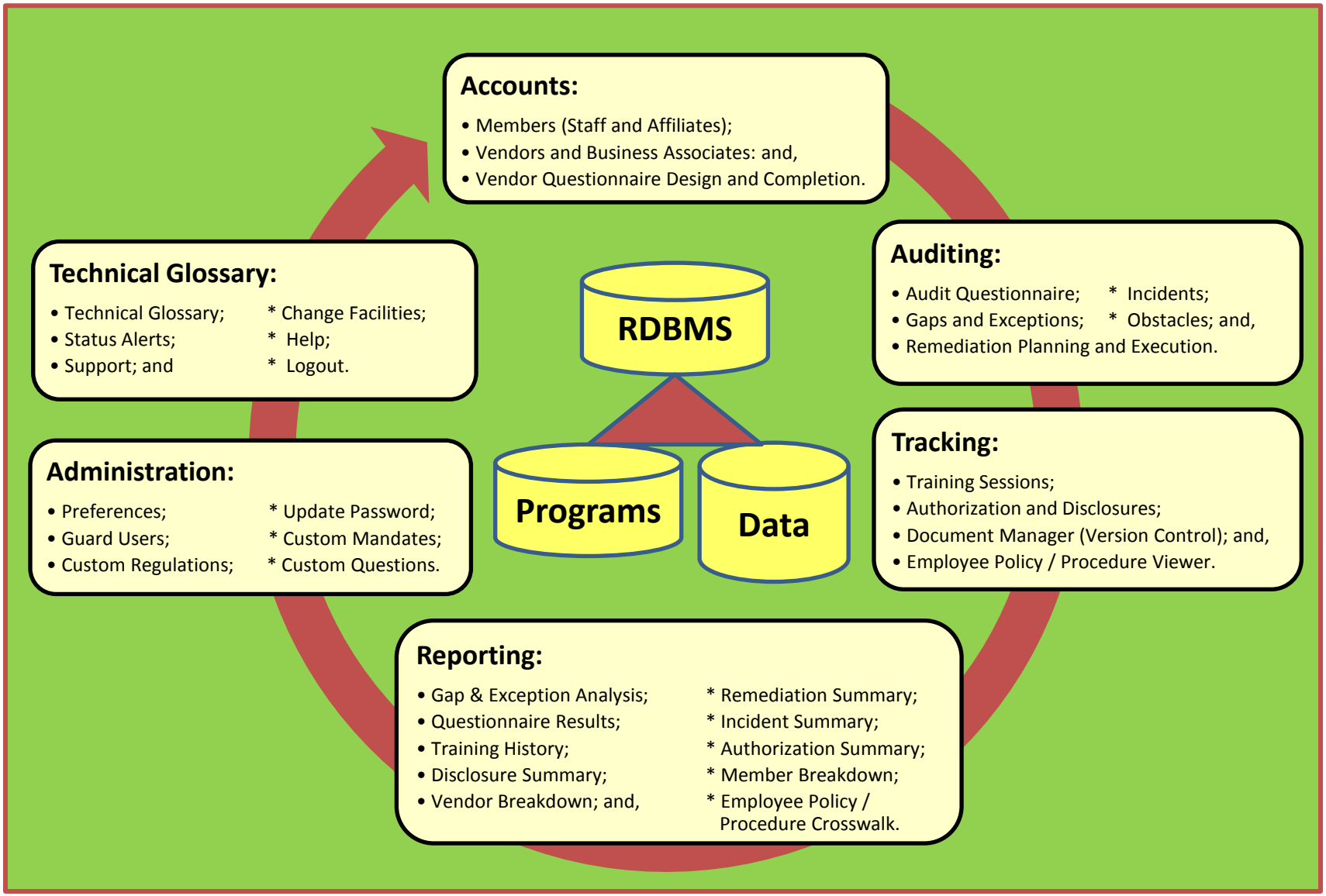
As you can see, penalties and loss of reputation can grow rapidly through repeated violations

Steps that lead to Achieving Compliance Goals and Objectives

- Perform a **Risk Assessment,** conduct a **Physical / Data Security evaluation**, and review **Emergency Response Plans** regarding compliance issues;
- Conduct a **Workflow Analysis** to uncover inefficiencies and Supply Chain flaws;
- Define **Gaps, Exceptions, and Obstacles** that must be Mitigated and Mediated;
- Establish **Direction / Project Plan** to resolve issues and gain approval;
- **Implement** Mitigations and Mediations, including: Compliance, Controls, Emergency Response Plans, and Incident Management procedures;
- Provide **Awareness and Training** to employees and business associates;
- **Achieve compliance** to HIPAA, ePHI, HITECH, and Final Omnibus Rule;
- **Achieve JCAHO certification**, leading to improved business and profitability; and,
- **Provide Implementation, Support, and Maintenance going forward**.

HIPAA Five Step Circle of Compliance

Healthcare Industry Workflow Management System Goals



Example of existing Workflow Management System

ITIL stands for:

Information
Technology
Information
Library

ITIL Five Phase approach to IT Service Support

1. Service Strategy,
2. Service Design,
3. Service Transition,
4. Service Operation, and
5. Continual Service Improvement.

ITIL Available Modules

1. **Service Strategy**
   - Service Portfolio Management (**available Services and Products**)
   - Financial Management (**PO, WO, A/R, A/P, G/L, Taxes, and Treasury**)

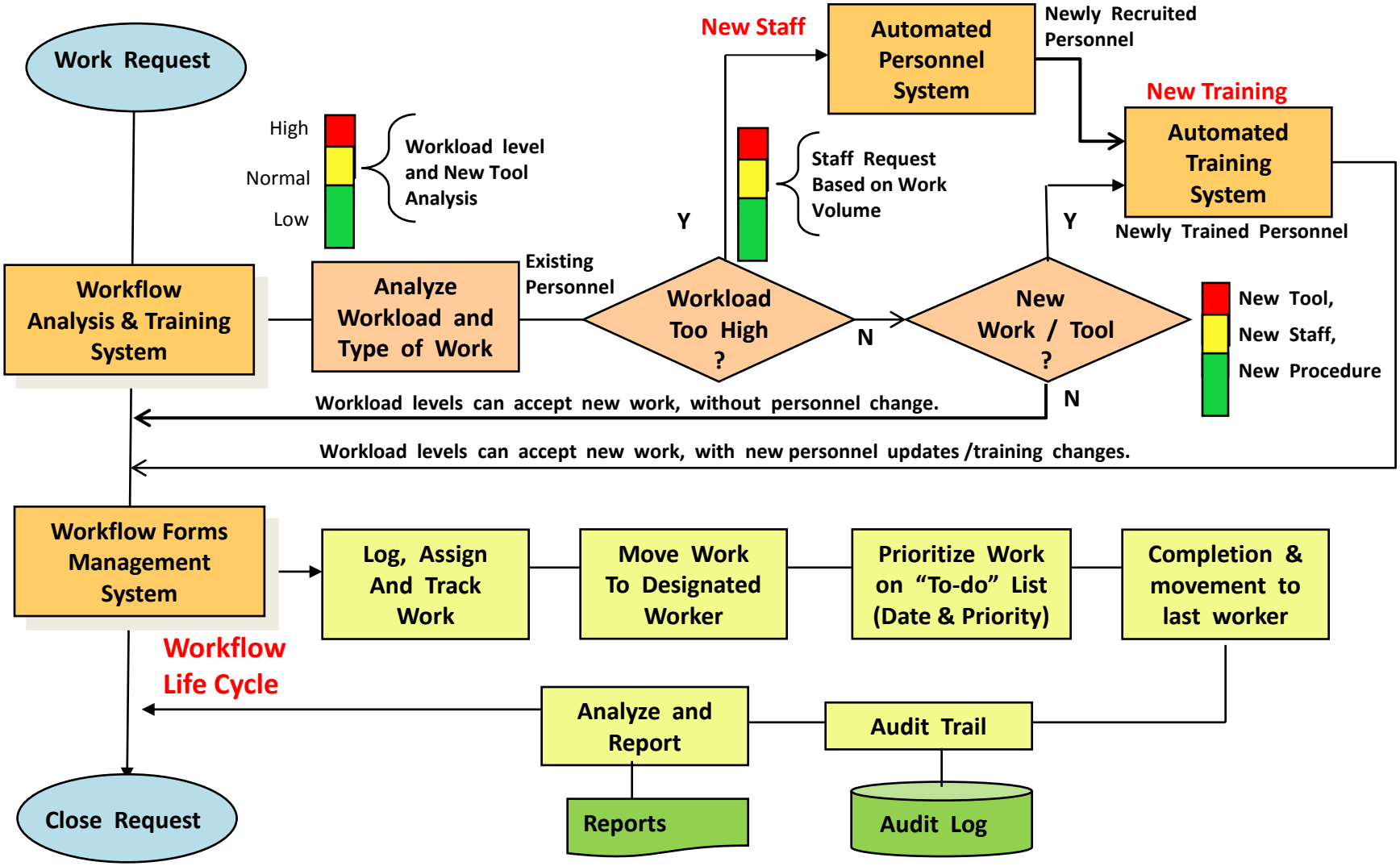
2. **Service Design**
   - Service Catalogue Management
   - Service Level Management (**SLA / SLR**)
   - Risk Management (**CERT / COSO**)
   - Capacity / Performance Management
   - Availability Management (**SLA / SLR**)
   - IT Service Continuity Management **(BCM)**
   - Information Security Management **(ISMS)**
   - Compliance Management **(Regulatory**)
   - Architecture Management **(AMS, CFM)**
   - Supplier Management **(Supply Chain)**

3. **Service Transition**
   - Change Management (**Problems & Enhancements**)
   - Project Management **(Transition Planning and Support)**
   - Release and Deployment Management (**V & R Mgmt**.)
   - Service Validation and Testing
   - Application Development and Customization
   - Service Asset and Configuration Management
   - Knowledge Management (**Training & Awareness**)

4. **Service Operation**
   - Event Management
   - Incident Management
   - Request Fulfillment
   - Access Management
   - Problem Management
   - IT Operations Management
   - Facilities Management

Workflow Management / Training System Interfaces & Flow

(Request through fulfillment, with staffing increases and training as deemed necessary)



Building a Workflow Management / Training System

- Mandated to insure patient safety (right medication and on-time delivery), staff training, and certification in gain compliance to regulatory requirements.
- Create and respond to a Needs Analysis Questionnaire to identify Gaps & Exposures, Obstacles, and to define deliverables, time lines, and scope.
- Review current forms, workflows, and controls.
- Identify personnel associated with forms processing.
- Redesign Forms and Workflow associated with forms, as needed.
- Develop Forms Data Base System.
- Implement Forms Management System functions and flows.
- Create User Interface to Forms Management System.
- Produce Management, Technical, and User Analysis Reports.
- Document Forms Management System.
- Supply Awareness and Training to staff, employees and associates.
- Roll-out Forms Management System / Training System.
- Support and Maintain Forms Management / Training System going forward.

Joint Commission on Accreditation of Healthcare Organizations (JCAHO) review

- **JCAHO** is a pro-active investigator, while HIPAA is an exception driven investigator;
- **Covers** Hospitals, Nursing Homes, Office-Based Surgery Practices, Home Care Providers and Laboratories, along with their Business Associates;
- **Most prestigious** Healthcare Industry Accreditation Organization;
- **Certification** assures patients and providers that the healthcare organization has achieved the highest standards required by the industry;
- **To achieve certification** both healthcare organizations and their staff members must be able to **demonstrate proficiency** across specific job competencies and compliance issues;
- Both Healthcare Organizations and their Business Associates must adhere to **regulatory requirements and competencies**;
- **JCAHO Certification** will help you achieve: a competitive edge; an educated staff; an improved ability to retain and recruit staff; improved morale; new business; a higher level of safety; and a safeguarded and compliant workplace.

Initial Physical Security Practices for Admittance to ER and Hospital.

Unrestricted Patient Movement to gain entrance to Emergency Room and Hospital:

1. Patients enter past Guards Desk (no verification or scan);
2. Patient waits for admittance in waiting area (unsupervised);
3. Patient is Admitted and Vital Signs Taken (ID Shown);
4. Patient goes to Finance where they are Identified and insurance papers validated (first true check of identity);
5. Patient waits to be called to go to Emergency Room where they are examined by staff; and
6. Patient is admitted to hospital, or treated and sent home;
7. Visitors gain access to Hospital to visit patient (no verification or scan);
8. Response to violent / criminal acts is slow and often no evidence is available.

Problem Analysis:

- **Lack of security at ER area can lead to Threat**:
  - Identification at Entrance;
  - Metal Scanner or Search for weapons;
  - Surveillance and Cameras for evidence;
  - Restrictive movement of patients.
- **Possible Weaknesses**:
  - Unidentified people accompanying patients;
  - Unrestrictive movement can lead to terrorism;
  - Possible threat to people and hospital reputation.
- **Possible Threats include**:
  - Terrorism and Active Shooter;
  - Deranged People acting out;
  - Disgruntled personnel; and
  - Civil Disorder.
- **Possible Repercussions include**:
  - Bombs and Guns;
  - Deaths and Destruction or property;
  - Damage to facilities causing outage of service to community;
  - Sanctions and monetary loss;
  - Loss of reputation; and
  - Loss of business and many law suits, with potential facility closing.

Benefits, Savings, and New Business possibilities

- **Learn** existing and new Healthcare Industry compliance laws and regulations;
- **Identifying audience** that must comply to Healthcare Industry regulations;
- **Risk Assessment** to define current gaps, exceptions, and obstacles impeding compliance;
- **Formulate direction** plan to achieve compliance and implement a Workflow Management System that improves efficiency and better safeguards patient information and services;
- **Achieve** Physical and Data Security requirements;
- **Better utilize Information Technology** to achieve goals and improve efficiency;
- **Adhere** to compliance requirements;
- **Update** Functional Responsibilities and Job Descriptions, as needed;
- **Fully Document** upgraded environment in Standards and Procedures Manual and Usage Guides;
- Implement **Awareness and Training** programs, as required;
- Achieve **JCAHO certification**; and,
- Utilize compliance upgrade and JCAHO certification to **advertise** the healthcare organization, **attract** new patient and insurance business, and **retain** and attract personnel who have **a high morale**.

Achieving Compliance Goals, Objectives, and Tasks to be performed

Goals and Objectives are:

- Use this document to help achieve **compliance** requirements;
- Obtain **HIPAA certification** based on compliance;
- Obtain reimbursement via "**Meaningful Use**" directive for electronic data conversion;
- Implement a **Safeguarded and efficient environment** that complies with all laws and regulations for both the Healthcare Organization and their Business Associates.

Tasks to be performed are:

- **Presentation** as a teaching tool and awareness vehicle for compliance issues;
- Stakeholder identification and **team formulation;**
- **Team Awareness**, Education, Work Plan, Assignments, and Reporting Schedule;
- **Risk Assessment** to define Gaps, Exceptions, and Obstacles;
- **Repair / Control Plan** to Mitigate Gaps & Exceptions, Mediate Obstacle & Impediments;
- **Project Plan** including deliverable's, schedule, resources, time line, and costs;
- Perform tasks to **certify** Healthcare Organization, Associates, and Supply Chain;
- **Perform tasks** needed to gain **compliance certification** (JCHOA Compliant);
- **Integrate** Workflow Management, Compliance Procedures, and Response Plans;
- Develop and publish all needed **documentation;**
- Provide Awareness and Educational **Training;**
- **Integrate** process within everyday functions performed by personnel; and,
- Provide ongoing **Support and Maintenance** going forward.

I look forward to working with you to achieve the goals of this proposal.

Points that should be remembered include:

- **The CEO is responsible** for producing a safeguarded and efficient environment that is in compliance with HIPAA, OSHA, NFPA 1600, and DHS regulations (at a minimum);
- Specific new healthcare regulatory requirements are identified in this presentation;
- "Meaningful Use" reimbursement for converting Medicare / Medicaid file conversion to electronic data can be as high as $40 - $60K per conversion
- The CEO can not delegate his responsibility, only share some responsibilities with insurance companies;
- Damages from lawsuits can run into the multiple millions and over all damages can exceed billions;
- Loss of reputation can result in the closing of the facility;
- Damages to the community can be extensive;
- Criminal and Civil charges can result in jail time and extensive monetary penalties; and
- Only you can take the initiative to implement a safeguarded environment that is in compliance with all regulatory requirements, while improving productivity and personnel morale. **"It is better to set the example than to be the example"**.

I can be reached via the following contact information:

Thomas Bronack, President Data Center Assistance Group, Inc. 15180 20th Avenue Whitestone, New York 11357	Cell Phone: (917) 673-6992 Email: bronackt@dcag.com

Thank you