Proposal to Healthcare Providers

On how to adhere to

- **Regulatory Requirements and ensuring a Safe Workplace**
- **(Related to "Patient Protection and Affordable Care Act – PPACA**

Including:

- **HIPPA, HITECH, ePHI and the Final Ombudsman Rule (Medicare / Medicaid).**
- **Workplace Safety, Security and Threat Elimination via Workplace Violence Prevention (OSHS, DHS, NFPA2600) and other mandated Laws and Regulations.**
- **Enterprise Resilience though Risk and Recovery Management Practices.**
- **Workflow Optimization / Employee Training Management.**
- **Workflow Optimization / Employee Training Management.**

Audience:

- **Hospitals, Clinics, Doctors Offices, and**
- **Businesses Associates with supporting Healthcare Organizations**

Prepared by:

Thomas Bronack, president
Data Center Assistance Group, LLC
bronackt@dcag.com | bronackt@gmail.com
Phone: (917) 673-6992
Website: https://www.dcag.com

Adhering to Healthcare Industry Regulatory Requirements

New laws and regulations governing the Healthcare industry require management to comply by September 23. 2013, or face sanctions, fines, and reputational damage. The new laws and regulations are related to the Patient Protection and Affordable Care Act (sometimes referred to as Obama Care) and designed to better protect patients and reduce medical costs. The new laws and regulations ensure patient physical security in the healthcare location or workplace; protect patient information from unlawful access, usage, and sale; and they apply to a wider range of media from paper based to social media devices.

The new laws and regulation **apply to** Healthcare Organizations (Hospitals, Clinics, Doctor Offices) and their Business Associates (any company or entity that provides services to Healthcare organizations, including vendors, service providers, and product companies. Both the Healthcare organization and their Business Associates must comply with the new regulations discussed in this article.

Implementing the new laws and regulations will **improve patient care** and reduce medical costs associated with redundant (or unnecessary) diagnostic testing, inefficient workflow practices that may result in patients receiving incorrect medications or late delivery of required medications needed to support patient care and reduce elongated patient hospital stays or treatments.

Some of the **benefits** that are hoped for include: remote diagnostic and patient care assistance via network communications; ability to treat cleansed patient medical information as a data mine that can be examined to plot trends and respond to medical alerts in a fashion that reduces or eliminates pandemic illnesses; and the implementation of a new paradigm relating to improved patient care at a reduced cost.

Using **technology** to cleanse patient medical information (no patient information just symptoms and the results achieved through responsive actions) will lead to trending information to provide the medical community with needed data to support test results or justify new developments. Combining the new use of Information Technology with patient information will lead to new medications and treatments to improve patient care, while improved communications and the use of patient information (**New Patient Freedoms** allow for the sharing of patient information when authorized by the patient or their representative) to obtain remote expert diagnose and treatment assistance.

Deliverables are necessary to achieve compliance.

This article provides Healthcare Industry personnel with a better understanding of the Laws and Regulations introduced to manage the medical industry and its patients.

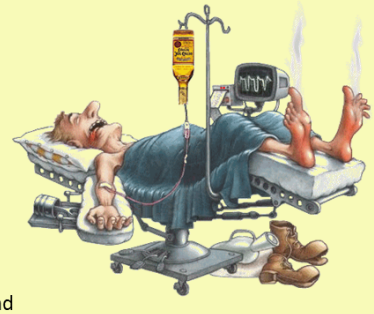
- **Define** the new and existing laws and regulations affecting the Healthcare industry and their Business Associates.
- Discuss **New Patient Freedoms** related to patient information sharing.
- Explain how to receive the **Joint Commission Accrediting Healthcare Organization** (JCAHO) certification and why it will benefit Healthcare Organizations.
- Suggest methods for performing a **Risk Assessment** including Risk Management, Auditing, and Incident Reporting.

- Formulate how better utilization of **Information Technology**, Data Management, and Access Controls can create a safeguarded and efficient environment better able to protect patient information while improving patient care.
- **Ensure that Service Level Agreements (SLA) and Recovery Time Objectives (RTO) meet the requirements of Recovery Time.**
- Determine how to develop and implement **Security and Emergency Response planning** needed to protect the Workplace, safeguard Patient Rights, and comply with regulatory requirements.
- **Creating** a project plan / road map to achieve Physical and Data Security.
- I assist in creating and **implementing Recovery Management** techniques covering Emergency Response, Disaster Recovery, Business Continuity, Risk Management, and Crisis Management.
- Assist in the design and implementation of an improved **Workflow Management System** to better protect the delivery of patient medications and billing.
- **Create documentation** defining new personnel Job Functions, Job Descriptions, Standards and
    - Procedures, and supportive Manuals, as needed.
- Develop and provide **Training and Awareness** processes as needed to become certified in the new laws and regulations.
- **Integrate** new procedures and compliance procedures within the everyday functions performed by the staff and business associates.
- Implement **Support and Maintenance** procedures going forward.
- Provide **periodic testing** and certification of compliance.

What is wrong with the Healthcare Industry and how can we fix it?

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

- **Patient Costs Soar, while Services Suffer:**
- **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**;



- Includes **Documentation** used to support patient services and respond to **incidents;**
- Includes **Awareness and Training** of staff and participants**;**
- **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.
- **Designed to** improve services and reduce costs through new technologies and procedures.

Presently, the Healthcare Industry and its medical practitioners are so afraid of **litigation** that they often order redundant tests that result in increased costs and delayed patient care and treatment, while Supply Chain vendors and in-house medication delivery procedures can result in patients not receiving their medication on time or even receiving the wrong medication. It is therefore imperative to create and implement **workflow** procedures that better respond to patient needs through delivery of the right medication at the right time. Tracking patient care and medications is essential to ensure that patients receive the best care possible, while billing is more efficient.

New Patient Freedoms allow patients, or their authorized representatives, to transmit their encrypted medical records to remote medical offices, or physicians, so that the patient's history is known, and additional testing eliminated, thereby providing better patient treatment and care by allowing consulting / new doctors to have access to past patient medical conditions and treatments.

As **Information Technology** improves it will become more important to allow remote assistance to supplement patient care. As these services increase, they will result in the development of new tools and technical procedures that improve patient treatment by faster and more informed response to patient needs. Improved medical collaboration through communications technology will result in the implementation of better understanding of patient medical conditions and the responses used to treat patients. Developing a data base of medical conditions and responses will provide improved detection and corrective action, while allowing for the examination of trending information to determine how best

to rate responses based on their success factor. In short, the use of Information Technology to provide patient care in the future will better safeguard data against corruption or illegal use.

Laws and Regulations affecting the Healthcare Industry

The laws and regulations can be understood in more detail through on-line search engines or through medical institutions, so only a brief description of them will be provided in this document.

The existing **HIPAA** (Health Insurance Portability and Accountability Act of 1996) was created to enhance awareness of patient rights and to safeguard the access and use of patient information.

HITECH (Health Information Technology for Economic and Clinical Health or 2009) was added to the HIPAA guidelines to include more stringent sanctions and fines for violation of HIPAA and HITECH rules and regulations.

ePHI (electronic Personal Health Information of 2009) was introduced to better protect electronically transmitted patient information from unauthorized access, use, or sale. It covers innovative technologies that were not mentioned in earlier regulations and includes compliance with the maintenance and access of medical information contained on paper, electronic devices, videos, audio devices, or any other form of electronic devices and communications affecting patient information.

Final Omnibus Rule (introduced 1/25/2013) was created to specifically state compliance guidelines and define the Final Privacy, Security, and Enforcement sanctions and fines that can be applied for failure to adhere to the new Healthcare Industry Laws and Regulations.

The **Meaningful Use** clause of the Final Omnibus Rule provides for reimbursement (from $40K to $60K) to healthcare providers for the conversion of their records to an electronic format that can be enforced through the new laws and regulations.

Workflow and the insurance that patients receive the correct medication at the right time is included in the laws as well and is meant to improve patient care by eliminating the delivery of wrong medications or missed medication deadlines.

These laws and regulations apply to healthcare organizations and their **Business Associates**, including service providers, consultants, and product manufacturers.

All people associated with the delivery of healthcare must comply with the new rules and regulations, and they should receive proper **training and certification** on their understanding and ability to respond to the new laws and regulations.

Although HIPAA and healthcare industry laws and regulations were not strictly enforced in the past, the new laws and regulations will be **aggressively enforced going forward** to encourage better patient care at a reduced cost to the government and patients.

To that end, **States Attorney Generals** can bring lawsuits on behalf of private individuals for breach of Privacy Rules or other clauses included in the new laws and regulations. Should this happen, the results could include sanctions, criminal and civil lawsuits, monetary fines, and the loss of reputation. All these negative outcomes could result in a greater loss than the implementation of compliance procedures, so it can be used as an aid in insuring healthcare industry compliance.

Who must comply with the new laws and regulations?

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.

As you can see, people are affected by the new Healthcare Laws and Regulations, so it is important to include the disciplines listed above in the planning and implementation process used to comply. Utilizing the combined knowledge of this audience will result in better plans, increased awareness, and faster implementation of compliance responses and recovery plans. The topics that should be discussed during planning session have to define and understand the laws and regulations associated with Administrative Safeguards, Physical Safeguards, and Technical Safeguards as listed below.

Areas affected by the New Compliance laws and regulations.

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).**

There are three major areas that need to be addressed within the new healthcare industry laws and regulations, they are:

- **Administrative Safeguards** – used to address how personnel are screened, hired, trained, assigned to a functional responsibility, allowed access to date, report and respond to incidents and audit exceptions, evaluated and rated on a periodic basis, and their contact with business associates (from definition through accreditation).

- **Physical Safeguards** – used to protect the facility, workstation use, workstation security, and device and media controls. These protections effectively limit physical access to locations and the equipment contained at locations, to authorized personnel only.

- **Technical Safeguards** – are applied by Information Technology and address Access Controls to data, Audit Controls to support compliance, Integrity of information and its used by the staff and business associates in compliance to regulations and patient requests, Person and entity recognition and authentication, and the Secure Transmission and Transportation of patient information.

Procedures must be upgraded to address the above areas to achieve compliance.

Penalties associated with non-compliance.

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

The sanctions and penalties associated with the new Healthcare Industry laws and regulation can be costly indeed, as shown above, but failure to comply can result in an even greater loss due to reputational damage or the failure to be able to provide the community with necessary medical care.

It has been shown that compliance with the new laws and regulations will result in improved morale through training and awareness, better retention of staff and clients, and the improvement of business by attracting new clients because of the organizations certified compliance response to the new laws and regulations. People and insurance companies would prefer to work with an organization that is certified, because it demonstrates competency of the care being provided, and the skills possessed by the staff. It also safeguards the decision maker by eliminating doubts associated with the level of care provided.

Improving the use of Information Technology will enhance the organization's profile, ensure data protection through access control, data management, and data recovery needed to support on-going operations even if a disaster event should occur. As more Information Technology usage is adopted to

support patient care and operations, it will become even more important to ensure that this service is available, thereby justifying the adoption of incident reporting, support, maintenance, recovery planning and implementation. Including Risk Management, Auditing, and Periodic Testing will ensure the continued supply of Information Technology to support organizational and patient needs.

How is compliance achieved?

The steps needed to achieve compliance with the new laws and regulations include the following steps:

- Provide management with a written **proposal and presentation** of their needs and the approach you recommend to achieving compliance.
- Gain **management approval**, budgetary authorization to implement and maintain compliance going forward, and strong management support of stated objectives so that personnel will understand management's commitment and their need to cooperate.
- Perform a **Risk Assessment** to uncover Gaps, Exceptions, and Obstacles impeding compliance.
- Conduct a **Physical Security** review to determine how to improve facility access and evidence collection.
- Conduct a **Data Security** analysis to define how data is defined, placed, accessed, used, transmitted, and transported. Also perform an investigation of encryption to protect data both internally and during transport electronically or physically.
- Conduct a **Workflow** analysis to determine how work tasks are generated, assigned, performed, validated, and recorded.
- Establish a **Direction / Project Plan** to resolve issues.
- Implement **mitigations and mediations** to eliminate gaps, exceptions, and obstacles that will result in compliance, control implementation, response plans, and incident management procedures.
- **Update** employee functional responsibilities and job description as needed.
- Fully **document** standards, procedures, and produce supportive manuals and materials.
- Provide **Training and Awareness** sessions and certifications for staff and participants.
- **Integrate** new standards and procedures within the everyday functions performed by the staff;
- Incorporate **Support and Maintenance** procedures to respond to problems, incidents, and enhancements; and
- Perform **periodic testing** and auditing of new processes to ensure continued compliance.

HIPAA - Five Step Circle of Compliance.

To assist organization and achieve compliance, HIPAA has developed a Five-Step Circle of Compliance that is used to:

1. Global Tracking.
2. Reporting and Visualization.
3. Compliance Management Tools.
4. Account Management.
5. Auditing and Remediation.

Following these steps will help ensure compliance with HIPAA and the new regulations and laws. The process includes Account Management; identification and reporting of Incidents and their tracking from origination through completion (with assigned personnel, the functions they performed, the amount of time needed to perform the functions, and the success of the resolutions they implemented); Auditing and Remediation validation; and Reporting.

The illustration below shows the components included in the HIPAA Five Step Compliance Circle.

HIPAA Five Step Circle of Compliance

Following this methodology will ensure compliance with HIPAA laws and regulations and allow for the easy identification and resolution of problems and incidents.

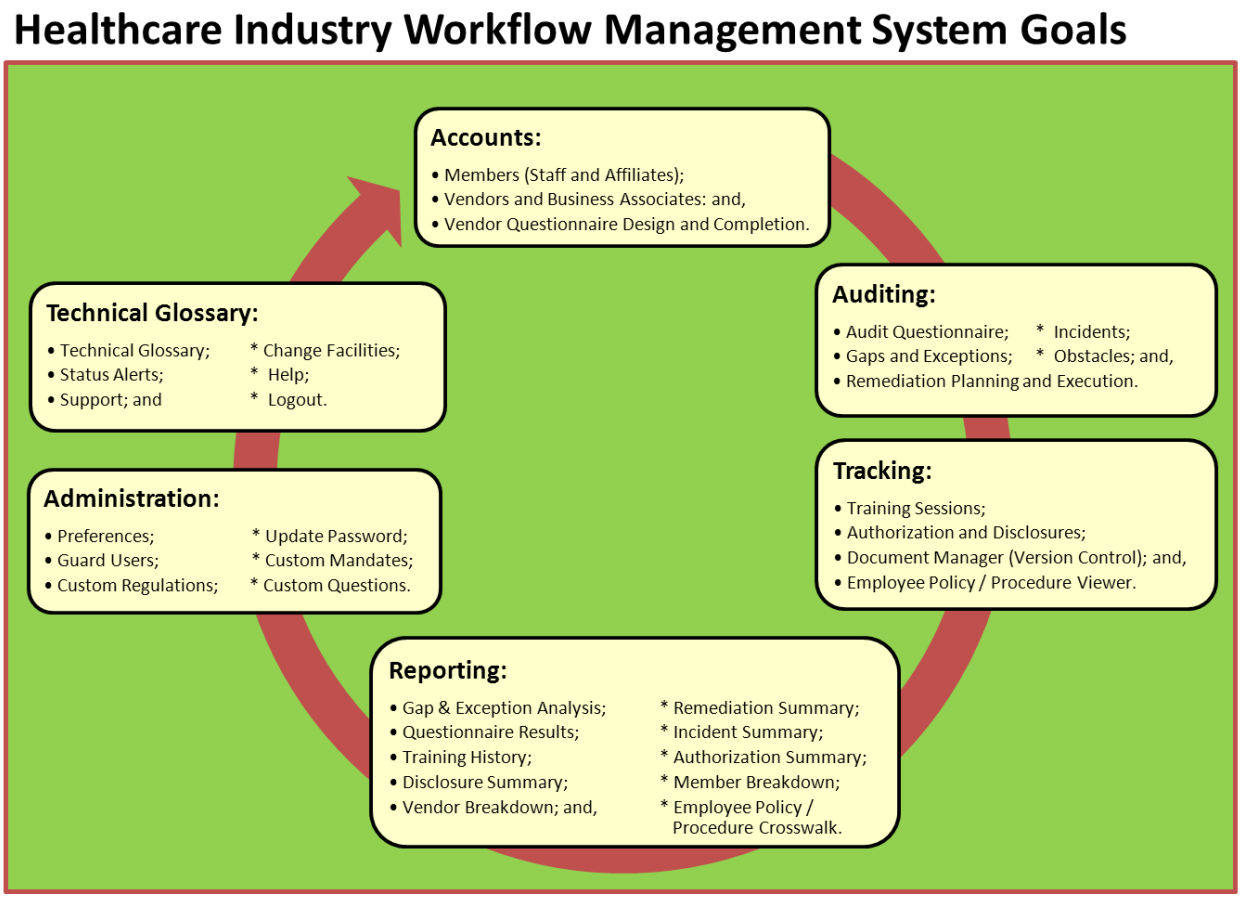
There are many vendor products that adhere to this process and many of them may be less expensive to implement than building a similar system of your own, but if your organization is different than most you may have to consider whether you want to develop a system of your own or purchase a vendor system.

Healthcare Industry Forms Management and Control System description

The HIPAA Five Step Circle of Compliance is a recommended approach by HIPAA, but it requires the creation and use of internal forms that will lead to automated compliance and easy attestation by executive management that the organization is adhering to the laws and regulations.

An illustration demonstrating how this is accomplished is displayed below.

Healthcare Industry Workflow Management System



The information that must be maintained by a Healthcare Organization to make complaints includes:

- **Accounts** – to list staff and affiliates (doctors, clinics, labs); Business Associates; and Vendors. Also, a Vendor Questionnaire is used to identify the vendor and its authorized staff, any other compliance information necessary to identify and authorize a vendor and certify their compliance.

- **Auditing** – including an Audit Questionnaire, Gaps and Exceptions, Obstacles and impediments, Incidents, Remediation Planning, and Remediation Resolutions.

- **Tracking** – including training sessions, authorizations and disclosures, document management. (Version and Release Management) and verifying that employees have read required policies.

- **Technical Glossary and Support** – to provide definitions of commonly used terminology, status alerts, change and management controls over facilities, support, help, and logoff maintenance.

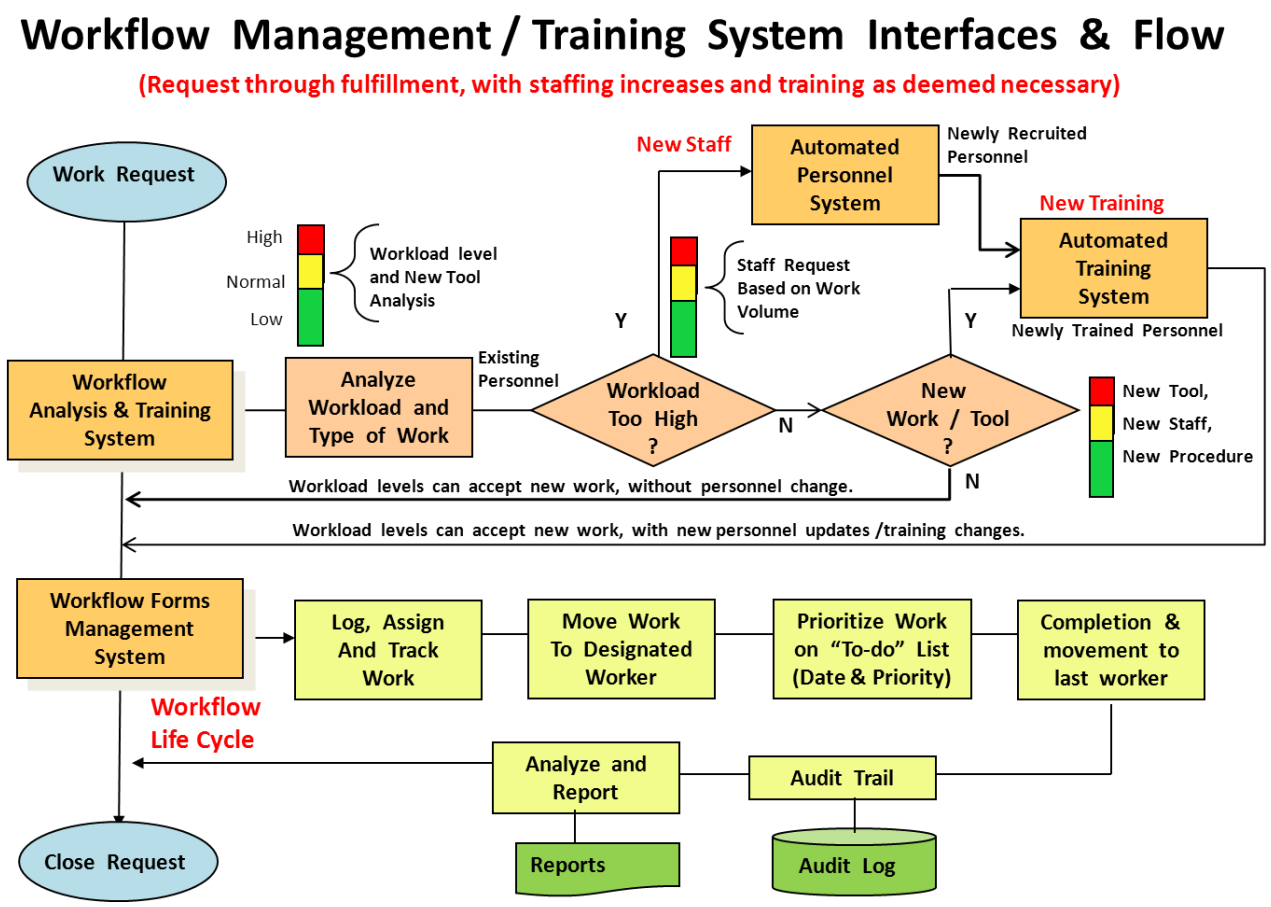
- **Administration** – User definitions, User ID's and Logon Password, Password Maintenance, Preferences, Custom Mandates, and Custom Regulations covering staff and guards.

Workflow Management, Recruiting, and Training System goals and objectives.

The new laws and regulations mandate training and awareness sessions to be delivered to the staff, affiliates, and business associates. Also, new workloads, loss of staff, and modern technologies or procedures may require recruitment and training. To achieve these goals, the following type of system should be considered for installation and use. It provides the following functions:

When Work Request are entered into the system in support of project staff requirements, new employees, workload volume, or new technologies and procedures they are examined by the Workflow Analysis & Training System and routed to an Automated Personnel System used to recruit new staff, or an Automated Training System used to orientate new employees, or provide training on new technologies or procedures.

Work Forms are passed to the Workflow Forms Management System where form validation, logging, routing, tracking until completion, and reported on. This process ensures that forms are understood, and the entered data has been validated. Reports help audit workflow and make improvements.



The steps that must be followed to implement a Workflow Management System include:

- **Create** and gather responses to a Needs Analysis Questionnaire to define laws and regulations, identify Gaps, Exceptions, and Obstacles to achieving Compliance, and define scope of deliverables, timelines, and costs associated with achieving compliance.
- **Review** current forms and workflow controls.
- **Identify personnel** associated with forms completion and processing.
- **Redesign** Forms Management Data Base to better reflect form information and flow needs.
- **Implement** the Forms Management System functions and flows.
- Create a **User Interface** between the Forms Management System and its Users.
- Product management, technical, and user Analysis **Reports**.
- **Document** Forms Management System and all associated manuals.
- Supply **Training and Awareness** programs to staff and participants to certify their understand of, and ability to comply with, the Forms Management System.
- **Roll-Out** Forms Management System throughout the organization.
- Provide **Support and Maintenance** going forward; and,
- Conduct **periodic reviews** to ensure that the Forms Management System is satisfying needs.

Safeguarding the Information Technology function and Business Locations

It is now becoming understood how important it is to protect the Information Technology function and location throughout the Healthcare Organization. Recent damage caused by Hurricane Sandy has illustrated the cost associated with salvage and restoration of services, but without a recovery plan chaos will prevail.

The next few pages will discuss how to perform recovery planning, site protection, salvage, and restoration. Steps leading to the creation of Recovery Plans include.

- **Management approval**, budget to create and maintain recovery plans, and dedicated support to ensure personnel contribute to the recovery planning and implementation process.
- **Risk Assessment** to define compliance requirements, gaps, exceptions, and obstacles impeding recovery goals.
- **Business Impact Analysis** (BIA) of physical locations and business units to define their criticality, resource requirements, and Recovery Time Objectives (RTO) to support operations and patient care.
- Review the **ability to support RTO** as defined in the client Service Level Agreement (**SLA**) and **BIA.**
- Identification of **Stakeholders and Participants** and the formulation of recovery teams at locations and within the Information Technology function.
- Provide **training and awareness** to team members.
- Selection of a **Recovery Management Tool** and definition of a Recovery Management Glossary
- of Terms to support a **common recovery management language**.
- Creation, testing, and **Proof of Concept** for recovery plans.
- Ensure **data recovery** can be achieved in support of Zero Downtime, Continuous Availability, and High Availability
- **Fully document** recovery management **standards and procedures**.
- Create **formal awareness and training** materials to support recovery management.
- **Roll out** recovery plans and certify that personnel know the functions assigned to them.
- Provide **Support and Maintenance** for Recovery Management.
- Provide **periodic testing** to validate recovery plans still function as required.

Following the procedures listed above will help you create a Workflow Management System that eliminates the greatest loss of productivity within any organization, that is, forms selection, completion, routing, and reporting on when the work is completed. It is recommended that you consider implementing a similar system within your organization.

Protecting Data through Access Controls, Backup, Recovery, and Vaulting

Data Security, Access Controls, Backup, and Recovery Practices.

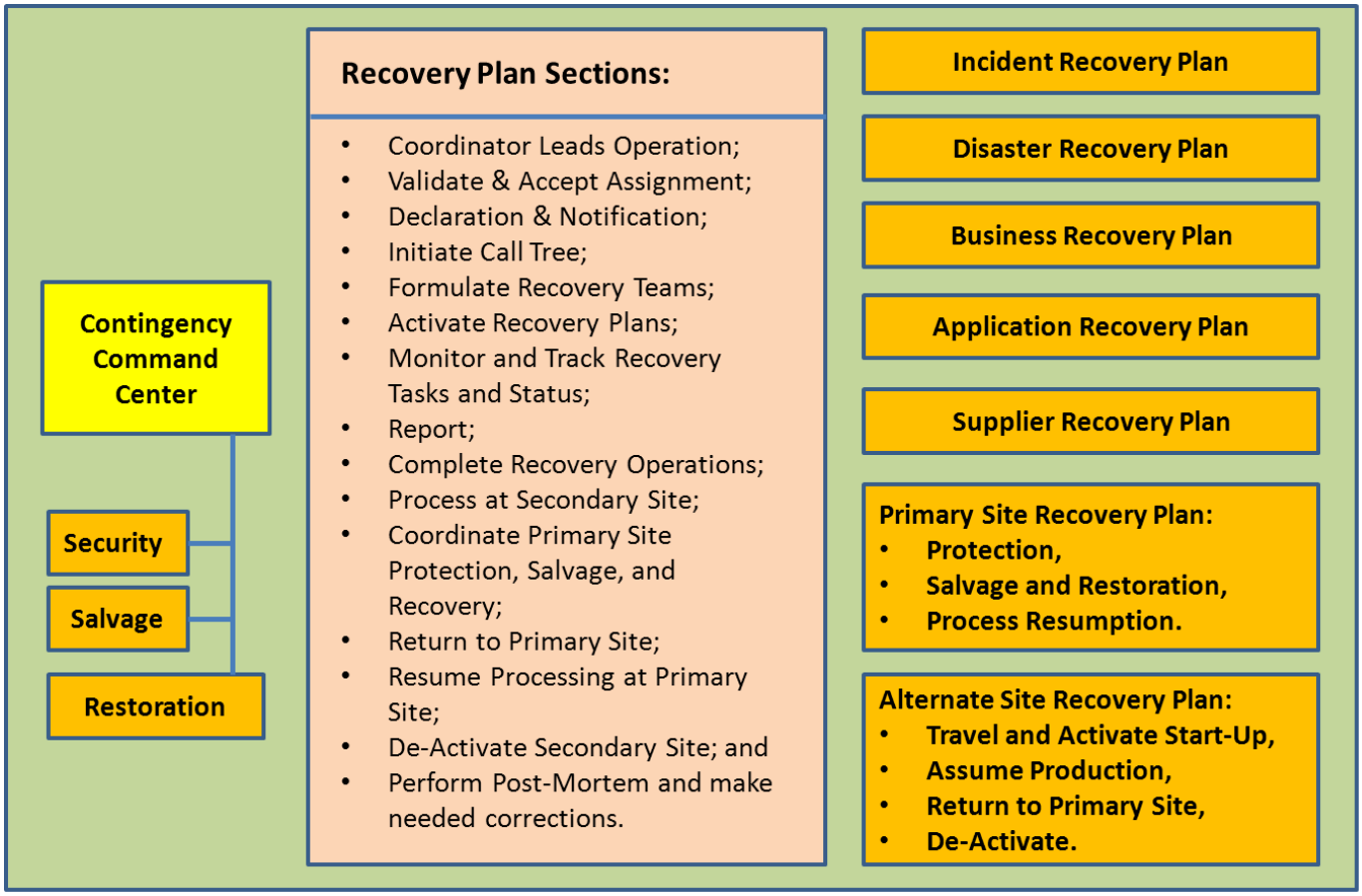
Mandated requirement to protect patient data:

1. Patient data must be **safeguarded** against unlawful use, sales, and transmission.
2. Patient data must be **available** when needed.
3. Patient data must be **encrypted** when transmitting off-site or between users.
4. "**New Patient Freedoms**" allow for the transmission of patient records when authorized by the patient or their representative:
    a. Between doctor's offices;
    b. To support remote doctor assistance;
    c. To accompany patient move to new location; etc.
5. **Medical Information trending** analysis can be performed after patient private information has been stripped from records being examined:
    a. Identify outbreak trending;
    b. To define past events leading to current illness;
    c. Establish concentric rings of defense against pandemics, etc.
6. For these reasons it has become necessary to better safeguard data and have it available when needed:
    a. Respond to "New Patient Freedoms" and future medical techniques;
    b. Protection of data and use of data for analysis, trending, and response;
    c. Increased use of data will require better data access, backup, and recovery;
    d. Utilization of new Information Technologies must be utilized to address the problem.

The illustration above provides an overview of mandated data protection requirements included in the new Healthcare Industry laws and regulations. Following these guidelines will result in protecting patient information from unauthorized access, use, sale, and loss.

"These data management procedures should be followed by all Healthcare Organizations."

Types of Recovery Plans and their Sections



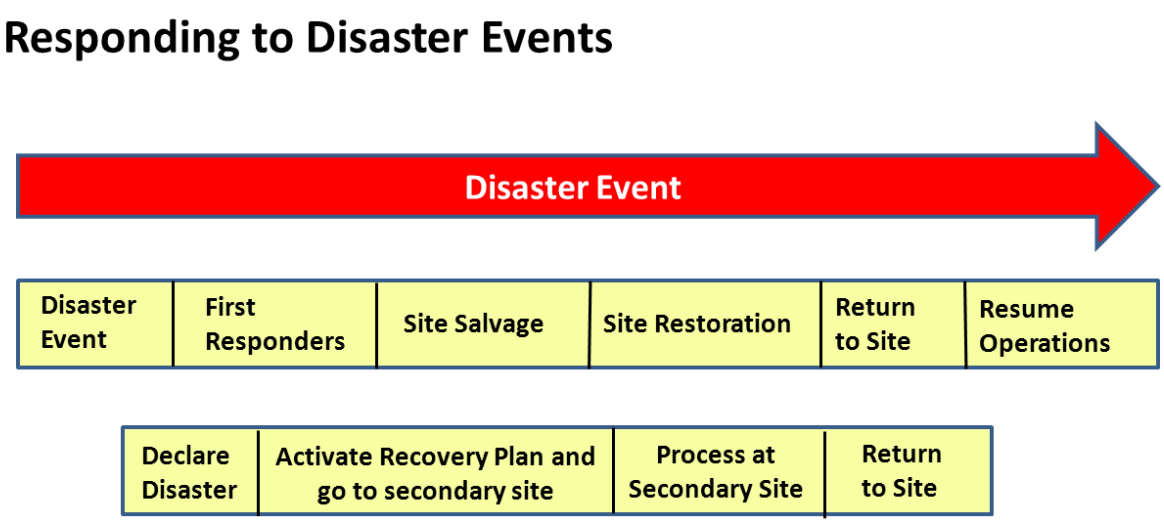
Once recovery plans are created, they must be identified, declared, and acted upon which requires interactions between end-users, command centers, and management. This is accomplished by most organizations through the following process.

Problems are detected by command centers (NCC for Network Problems, OCC for Operations Problems, ICC for Incidents) and reported to the Help Desk. The Help Desk records the problem and initiates problem resolution efforts. If resolution efforts fail, the Help Desk will select a Recovery Plan that matches the failure and notifies the Contingency Command Center (CCC) of the disaster event.

The Contingency Command Center (CCC) will validate the disaster event and notify the Contingency Coordinator associated with that recovery plan. The Contingency Coordinator will initiate the recovery plan by calling recovery team members and starting recovery operations. The CCC will coordinate recovery operations with the Emergency Operations Center (EOC) which is established when a disaster is declared. The EOC will coordinate business operations and communicate disaster event status with Executive Management. Executive Management is responsible for communication recovery status to the clients and outside world.

While recovery is responsible for shifting processing from a primary to secondary site, it is important to repair the primary site so that normal processing can be resumed.

Security, Salvage, and Restoration procedures



Site Security, Salvage, and Restoration is initiated when a disaster event occurs and is responsible for protecting, salvaging, and repairing the primary site in preparation for the production staff returning to the primary site to resume normal production operations. Their function begins when the First Responders declare the site clear for repair and reoccupation.

Site security is initiated immediately after a disaster is declared so that personnel are safely evacuated and building safety is provided. Security also ensures equipment, supplies, or other critical business information is not taken from the premises, because espionage can take faces or opportunists can seize the disaster event to illegally acquire business valuables. Company security coordinates activities with the local police department.

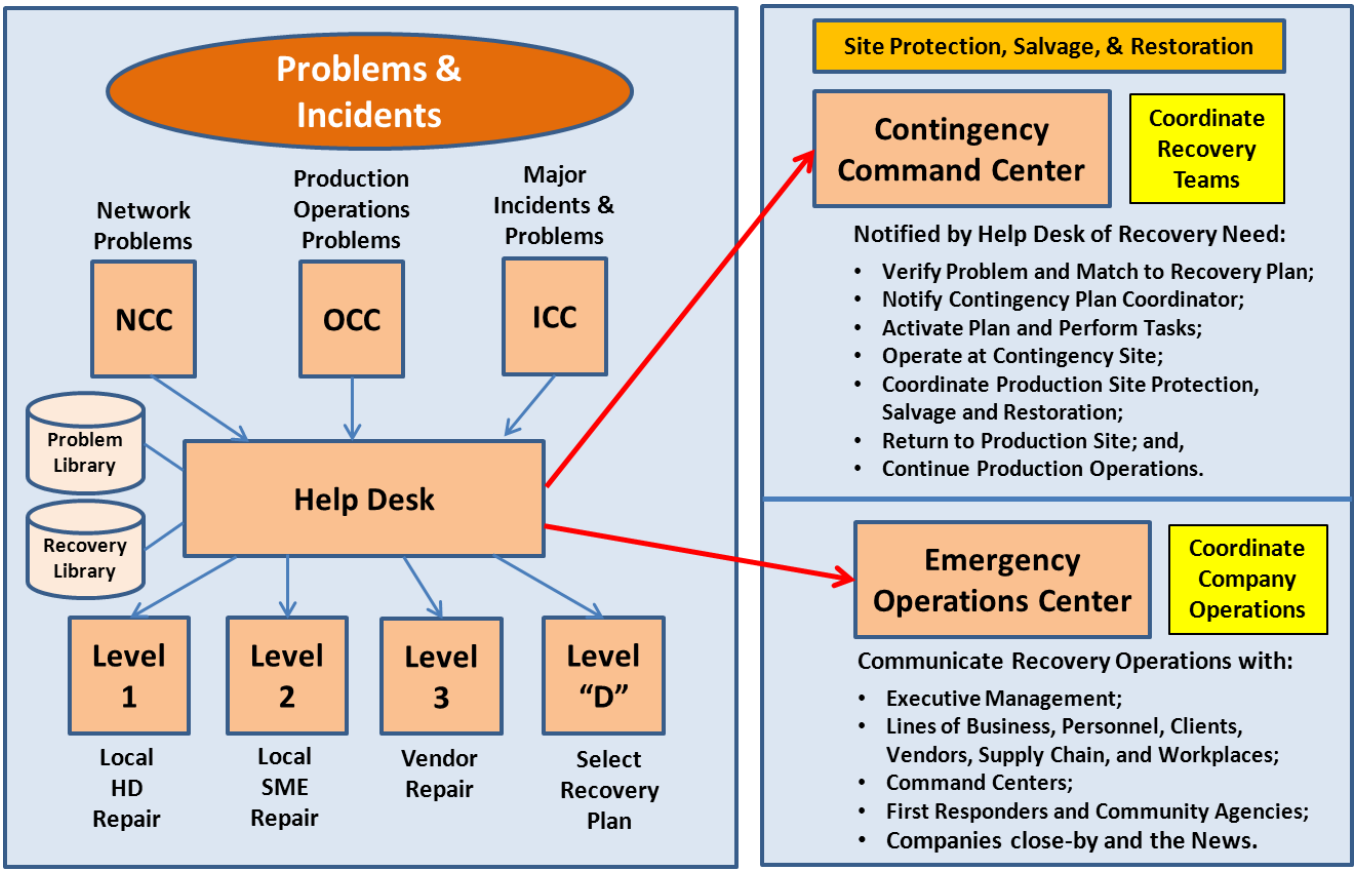
First Responders (consisting of the police, fire department, and emergency medical technicians) will perform their tasks immediately upon arrival on the scene. In cases, the building or affected area will be cordoned off which would interfere with normal business operations. You can usually be assured that the crime scene, or affected area, will be off-limits for multiple hours so the initiation of recovery plans should occur immediately when first responders are called to a business location.

Salvage and Restoration for sites is accomplished by companies like **ServePro** who are contracted to clean the affected area, salvaging any equipment or other business documents that may have been damaged, and then performing restoration activities needed to allow for the return of personnel after a disaster event.

By **combining Enterprise Resiliency with Salvage and Restoration** organizations, it may be possible to quicken recovery operations by having a partner who can better protect, salvage, and repair a location suffering from a disaster event because they helped develop the recovery plan and have participated in

recovery plan testing. Utilizing companies like ServePro in a partnership type of arrangement will enhance recovery planning and operations because they have a unique perspective on how a disaster can affect a company's operations and how long it normally takes to recovery a primary site after a disaster event.

Activating and Coordinating Disaster Recovery Plans



Disaster Recovery Plans can be initiated by the Help Desk when normal recovery actions cannot resolve the encountered problem or incident. The Help Desk would record the problem and the results of problem circumvention procedures, then they would first try to repair the problem themselves (Level I) or escalate the problem to the Subject Matter Expert (SME) responsible for the failing component (Level II). If the SME cannot resolve the problem, it is escalated to the failing components Vendor (Level III). If all repair attempts fail, the Help Desk will escalate the problem to Level "D" and declare a disaster event has occurred. The Help Desk then refers to its library of Recovery Plans and picks the plan that best responds to the disaster event. The Help Desk then contacts the Contingency Command Center who validates the recovery plan is appropriate to the disaster encountered and then they contact the Contingency Coordinator related to the plan.

The **Contingency Coordinator** would activate the recovery plan and perform all tasks contained in the plan from notification through relocation to the secondary site and the resumption of production processing at the secondary site. Once the primary site has been repaired and is ready to receive

personnel and resume normal production, the Contingency Coordinator will manage the return to the primary site and the resumption of normal production processing.

The **Emergency Operation Center** (EOC) coordinates business operations to minimize the impact of the disaster and communicates with Executive Management on the status of the disaster event, while Executive Management is responsible for communicating with clients and the outside world on when normal business operations will be resumes and the extent of the damage suffered during the disaster event.

An illustration of the people involved with recovery operations is provided below, while Physical Recovery Operations and Logical Recovery Operations illustrations are provided on later pages to demonstrate the "**End Goal**" associated with achieving Enterprise Resiliency and Corporate Certification.

Physical Security and the problems that failure to implement can cause.

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.

Implementing **Physical Security** within a Hospital or Healthcare Organization may appear difficult, but not implementing safeguards will result in greater problems and disaster events that could cause harm or death to personnel and the interruption of community services.

The Healthcare Organization should consider the above information and decide upon an approach to implementing Physical Security. **At a minimum**, CCTV should be used to identify people entering the complex and support the gathering of evidence should a disaster or illegal event occur. Remember you cannot prosecute without evidence, and evidence can also be used to correct uncovered problems.

Physical Security has a **low cost but delivers a huge return** on investment. It is the front line of protection for any organization and works hand and glove with First Responders, especially the police and fire department to help protect assets and personnel.

Obtaining Health Care Industry Certification via JCAHO

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) is the largest and most prestigious Healthcare Certification organization. It takes a proactive approach to certification, while HIPAA has been an Exception Based reviewer of compliance in the past. With the new laws and regulations, HIPAA has stated they will be more aggressive in ensuring compliance, which makes it even more important to receive certification from an independent source.

The services provided by JCAHO include:

- **Pro-active investigation** of Healthcare Industry compliance.
  Covers Hospitals, Nursing Homes, Office-Based Surgery Practices, Home Care Providers, Laboratories, and Business Associates.
- **Most prestigious** Healthcare Industry Certification firm.
  Certification assures patients and providers that healthcare organizations have achieved the highest standards required by the industry.
- **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; and,
- **JCAHO** certification will help achieve a competitive edge, educated staff, ability to retain and recruit staff, generate new business, achieve a higher level of safety, and prove compliance.
    - **JCAHO** certification will help generate new business and retain current business because it shows that the organization meets or exceeds industry's best practices.

The Benefits, Savings, and New Business Possibilities achieved through JCAHO certification include:

- **Learning about** existing and new healthcare industry compliance laws and regulations.
- **Identify audience** that must comply with regulatory requirements.
- Perform a Risk Assessment to define gaps, exceptions, and obstacles impeding certification.
- Formulate a **direction plan** to achieve compliance and implement Workflow Management that.
    - improves efficiency and better safeguards patient information and services.
    - **Better utilize Information Technology** to achieve goals and improve services.
    - **Update** functional responsibilities and job descriptions.
- **Fully document** upgraded environment in Standards and Procedures Manual and Usage Guides.

- Implement **Awareness and Training** programs, as required.
- Achieve JCAHO certification.
- 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.

You can see that there are benefits associated with complying with the new healthcare industry laws and regulations and obtaining JCAHO certification. It will result in a more efficient and safeguarded environment that will help retain existing staff and business, while attracting inexperienced staff and business going forward.

Steps needed to achieve compliance.

The following steps must be taken to achieve compliance.

- **Present** new laws and regulation requirements to the healthcare organization and its business associates.
- **Identify Stakeholders** and participants and formulate compliance teams.
- Provide team members with **initial Awareness Training**.
- Formulate a **Project Plan** to achieve goals (including tasks, resources, scheduling, costs, and deliverables).
- Define **reporting schedule** to track progress and respond to encounter problems.
- Conduct a **Risk Assessment** to uncover gaps, exceptions, and obstacles.
- Develop a plan to **mediate / mitigate** gaps, exceptions, and obstacles.
- **Implement** compliance requirements.
- **Update** personnel functional responsibilities and job descriptions.
- Develop and publish all needed supportive **documentation materials**.
- Provide **formal Awareness and Training** as needed.
- **Integrate** new functions within the everyday procedures performed by personnel.
- Provide ongoing **support and maintenance**.
- Create a plan to **periodic test compliance**; and
- Obtain **JCAHO certification.**

Achieving compliance will reduce the chance of a disaster causing extended outages and can result in saving lives and operations. It will improve the organization's reputation with the community and can result in the generation of new business and improved profitability. All these benefits justify going forward by complying with the new laws and regulations affecting the healthcare industry. Good luck in your endeavor.

About the Article and the Author

Adhering to Healthcare Industry Regulatory Requirements

New laws and regulations governing the Healthcare industry have been recently upgraded and will require management to comply by September 23. 2013, or face sanctions, fines, and reputational damage. The new laws and regulations are related to the Patient Protection and Affordable Care Act (sometimes referred to as Obama Care) and are designed to better protect patients and reduce medical costs. The new laws and regulations were framed to ensure patient physical security in their workplace or healthcare location; protect patient information from unlawful access, usage, and sale; and applies to a wide range of media from paper based to social media devices.

It is hoped that implementing the new laws and regulations will improve patient care and reduce medical costs associated with redundant (or unnecessary) diagnostic testing, inefficient workflow practices that may result in patients receiving incorrect medications or late delivery of required medications needed to support patient care.

Benefits that are hoped for include remote diagnostic and patient care assistance via network communications, ability to treat cleansed patient medical information as a data mine that can be examined to plot trends and respond to medical alerts in a fashion that reduce or eliminate pandemic illness. As technology is applied to cleansed patient medical information (no patient information just symptoms and the results achieved through responsive actions), it will lead to trending information that would provide the medical community with needed information to support test results or justify new developments.

This article is designed to assist in Healthcare Industry personnel better understand what actions are mandated in the new laws and regulations and how best to respond to them.

Thomas Bronack Bio.

Tom is a Certified Business Recovery Professional (CBRP) from DRII with a strong Compliance and

Recovery Management background. He has over 30 years of technical, managerial, sales, and consulting experience implementing safeguarded environments that comply with business/regulatory requirements. He is adept in planning and improving the efficiency of data processing systems/services by optimizing information technology productivity through automated tools, quality improvements, procedures, documentation, and training. Tom has presented materials and conducted workshops at IFSA, ISACA, ISSA, ACP and CPE User Groups and is presently on the Board of Directors of the NYC Metro Chapter of the Association of Contingency Planners and serves as the Director of Vendor Relations. He can be reached via the contact information listed below.

Thomas Bronack
Cell: (917) 673-6992
Email: bronackt@gmail.com
Web Site: www.dcag. com

