Healthcare Institutions face Challenges with Data Privacy Regulations – Government Mandated Compliance Requirements.

1. Introduction

Data Leak Prevention (DLP), i.e. protection of confidential data/information from unauthorized disclosure and/or use has become one of the biggest and most challenging security issues that is affecting Medical & Pharmacy Institutions, Medical and Healthcare Providers, Medical Practitioners and Medical Insurance Carriers alike.

Government regulations for protection of confidential information such as HIPAA-HITECH, PII, PCI, FERPA are mandatory Compliance requirements for all Medical & Pharmacy Institutions and Healthcare Training Centers.

For Medical & Pharmacy Institutions or Healthcare Training Centers, it is a mandatory requirement to comply with the following three regulations;

1. **Federal Educational Rights and Privacy Act (FERPA)** is a federal law designated to the privacy of student educational records. By law every educational institution is required to protect student educational record from unauthorized disclosure. This law requires protection of the (following information;

    a. **Academic Records** – This includes all educational records such as classes and coursework subjects, credit units taken, grades and GPA, semester information, degrees or diplomas earned, etc.

    b. **Student's Personal Information** – This includes information such as student's Name, Address, Student Identification No., Date of Birth, Age, Sex, Ethnicity, Nationality, Payment Information, etc.

2. **Health Insurance Portability and Accountability Act (HIPAA-HITECH)** is another important federal law that is mandatory for all entities involved in medical and healthcare fields. This law requires protection of the following information;

    a. **PII (Personally Identifiable Information)** – This includes data/information that can uniquely identify an individual, such as Name, Address, Date of Birth, Social Security No., Phone No., Medical Record No., Account No., etc.

    b. **ePHI (Electronic Protected Health Information)** – This includes data/information such as Personal Health Records including medical reports, laboratory test reports, medical prescriptions, medical diagnosis, surgical reports, etc.

3. **Payment Card Industry (PCI)** is another important federal compliance regulation that is mandatory for all entities involved in medical and healthcare fields. This compliance regulations requires protection of the following information;

    a. Credit Card No., Expiration Date, Card Security Code, PIN No., holder's Name, Address, Social Security No., etc.

Additionally, every state has its own specific regulations for data security that must be adhered to by all Medical & Pharmacy Institutions and Healthcare Training Centers.

2. Changing Nature of Data Security Threat

Until recently, many Hospitals, Clinics, Healthcare Providers, Healthcare Software companies, Medical & Pharmacy Institutions have focused on external threats, taking steps to guard against security breaches including viruses and malwares.

But more recently, internal threats have posed an even greater risk. Data loss/theft due to insider **accidental or malicious activities** is becoming more and more prevalent than ever before.

HIPAA-HITECH and other Government regulations are only getting stricter and closely watching entities and organizations in an effort to protect patient/client confidential information. Hospitals, Clinics, Healthcare Providers, and Medical & Pharmacy Institutions need to secure precious data and patient/client information in the best possible way while at the same time increasing productivity and reducing operating costs.

3. GhangorCloud 'Information Security Enforcer' (ISE) for Healthcare Institutions

GhangorCloud is an industry-recognized leader that has built a 4th Generation Data Leak Prevention (DLP) solution for the Healthcare Industry. GhangorCloud' DLP product has won several industry awards including the most ***prestigious Frost & Sullivan "Excellence in Technology Innovation Award – 2009".***

GhangorCloud's Information Security Enforcer is a ***Real-time Data Leak Prevention*** solution for detection and prevention of potential leak or unauthorized disclosure of data protected under the FERPA, HIPAA-HITECH and PCI compliance regulations.

GhangorCloud's Information Security Enforcer DLP solution has been built from the ground up to cater to the HIPAA-HITECH compliance mandate described in HIPAA guidelines as follow;

1. Determine which individuals are authorized to work with ePHI in accordance with an **Identity & Role-based access approach (HIPAA §164.308.a.3)(A)**.

2. Ensure the verification of the individual or entity who is authorized to access ePHI and that the identity is correctly bound to a unique user identification ("sign-on") for access to **ePHI (HIPAA §164.308.a.4)(A), (HIPAA §164.312.a.1)(R), (HIPAA §164.312.d)**.

3. Ensure appropriate access controls mechanisms for authorized users' access to any ePHI. For systems with the capability, require strong electronic authentication, such as sufficiently complex passwords or use of other encryption key mechanisms to access systems containing **ePHI (HIPAA §164.308.a.5)(A)**.

4. Establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals or entities who have terminated or no longer are authorized to access **ePHI (HIPAA §164.308.a.4)(A)**.

5. Carefully manage system administrator accounts to ensure the accounts are used for only specific system administration functions. The number of these accounts should be kept to a minimum and provided only to personnel authorized to perform identified functions. Passwords or other authentication measures should be changed upon the termination of systems personnel who accessed these accounts.

6. Log activities performed by system administrator accounts and monitor logs on a regular basis **(HIPAA §164.308.a.1)(R), (HIPAA §164.308.a.5)(A).**

3.1 Identity & Role based Data Use (per HIPAA regulations)

GhangorCloud Information Security Enforcer enables ***Identity and Role Based Data Leak Prevention*** - the Identity and Role based DLP paradigm built from ground up to emulate the organizational structure of Healthcare Service Providers, Hospitals, and multiple parties in the Healthcare Service Chain.

GhangorCloud has been acknowledged by the industry as the pioneer of its **"Identity and Role Based DLP Paradigm"**. The Information Security Enforcer provides out-of-the-box integration with Active Directory, LDAP and RADIUS Servers to leverage the pre-existing data in the enterprise. The Information Security Enforcer provides an extremely easy GUI interface to "Point and Click" to automatically get connected to the Active Directory and LDAP servers.

Additionally, it has interfaces to Hospital Employees and Human Resource applications Database. This allows GhangorCloud' product the unique ability to create the most sophisticated Role and Responsibilities based DLP environment which is 'Tailor Made' for Healthcare Service Industry.

3.2 Automated Policy Generation (per HIPAA regulations)

As mentioned above, GhangorCloud' product has been designed and built grounds-up based on **a unique Roles-Responsibility based Policy Synthesis paradigm** that **automates** most of the tedious and error-prone manual policy setting process. In fact GhangorCloud is the very first DLP solution that has one of the **most powerful Automatic Policy Synthesis Engine specifically conceived for Data Leak Prevention style of Policy Generation and Enforcement**.

Policies can be generated to Control Access rights, to Restrict where a particular healthcare personnel or group of healthcare personnel can or can not share and/or disclose sensitive healthcare data (e.g. PII, ePHI related data) of a particular type and/or modality, to transfer or move sensitive data from unauthorized or Compliance violating locations, etc.

The Syntax and Semantics of Policies are very human friendly and very easy to understand by the Security Administrator.

GhangorCloud Information Security Enforcer utilizes HIPAA code sets (e.g. HCPCS, ICD-9, LOINC, and NDC) as built-in sophisticated 'Ontologies' to prevent patient data from inadvertently leaving the organization.

Domain Ontologies: Several domain specific Ontologies for PCI-DSS, HIPAA-HITECH, Pharmaceutical, Educational-FERPA, etc are pre-packaged with the system while additional healthcare related Ontologies can be ingested from other preexisting healthcare management software systems via interfaces for 3rd party Ontology ingestion. Furthermore, existing or newly

ingested Ontologies can be modified and customized via a graphical user interface, as per the needs of an enterprise.

3.3 Automated Alerts, Notifications and Workflow (per HIPAA regulations)

ALERTS NOTIFICATION and WORKFLOW are two of the strongest aspects of GhangorCloud' product. The GhangorCloud' product has very elaborate and comprehensive mechanisms that include;

- Administrator's ALERTS and NOTIFICATIONS that empower the IT Security Administrator in hospitals, clinics and other healthcare organizations to 'proactively' take decisions to avert a possible DLP scenario in real-time as soon as the system detects a potentially unauthorized data transaction.
- Manager's ALERTS and NOTIFICATIONS in compliance with HIPAA-HITECH requirements that empower the healthcare Manager / Supervisor to receive proper Event Information as Pop-Ups to be able to do real-time forensic and decide whether to ALLOW or DISALLOW (or take any other action) the end user's action.
- End user's ALERTS and NOTIFICATIONS that give Real-time prompt and WARNING to the end user alerting them that their invoked action may cause a potential Data Leak and hence empowers the End User to take immediate corrective measures such as ABORT, CANCEL, PAUSE, etc.
- GhangorCloud Information Security Enforcer embodies a very comprehensive WORKFLOW mechanism that enables it to MONITOR and TRACK step-by-step any DLP INCIDENT or EVENT from its beginning to its CLOSURE. Multiple parties who may be involved in the Decision Cycle can track the status of an OPEN INCIDENT or EVENT till its CLOSURE.

GhangorCloud' product has built-in mechanisms for very comprehensive FORENSIC ANALYSIS. It ha the capability to 'proactively' and 'automatically' identify sensitive and confidential HIPAA, PII, PCI and FERPA data whether it is stored in an authorized location, or it is being disclosed and used in unauthorized fashion, or it is being transferred in unauthorized ways. The Forensic Capabilities on GhangorCloud' product allows both Proactive Forensic Analysis and Historical Forensic Analysis. Very robust HIPAA, PCI, PII and FERPA content analytic algorithms and behavior pattern analysis methods are incorporated in the GhangorCloud Information Security Enforcer product to give unparalleled FORENSIC abilities.

4. Summary:

GhangorCloud Information Security Enforcer DLP product is 'tailor made' for protection of confidential healthcare data and information. The Information Security Enforcer is an ideal solution for the complex data security and privacy challenges faced by Medical & Pharmacy institutions, hospitals, pharmacies, clinics and other healthcare providers.

Built-in the Information Security Enforcer is the most advanced Semantic Analysis and Data Protection mechanisms that can automatically and in real-time identify and protect confidential data as per the HIPAA-HITECH, PII, PCI and FERPA regulations.

GhangorCloud Information Security Enforcer DLP product represents a new generation of Data Leak Prevention technology that is able to analyze, classify, recognize, and secure unstructured information in a way that is fundamentally different from existing technologies and methods.

GhangorCloud Information Security Enforcer DLP product can be deployed across any healthcare provider's network quickly, and can deliver superior results in terms of both accuracy and maintainability. The ability to automatically identify content, automatically classify it, generate security policies in real-time without requiring constant tedious manual intervention, and provide real-time protection against purposeful evasion drastically cuts down the cost of the DLP system both in terms of Capex and Opex. GhangorCloud Information Security Enforcer DLP product drastically reduces the Total Cost of Ownership (TCO) and headache for the IT.

GhangorCloud is the leader in the emerging next generation enterprise information security & compliance market. To schedule a demonstration please contact: info@GhangorCloud.com

CONTACT
GhangorCloud, Inc.
2001 Gateway Place
Suite: 710 West Tower
San Jose, CA 95110
www.GhangorCloud.com

How to get started:

GhangorCloud understands that every enterprise has its own unique data security needs. GhangorCloud's team of Data Loss Prevention experts and its Value Added Distributors will work with you to understand your unique data security requirements and priorities. Please contact GhangorCloud to get started, email info@GhangorCloud.com.