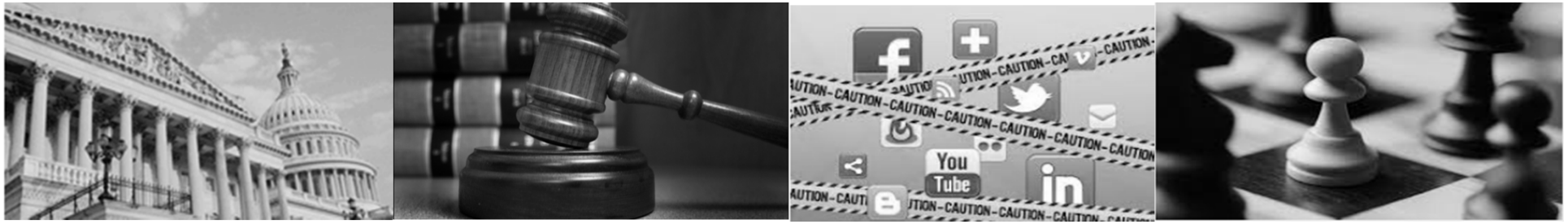


Monitoring, Measuring and Mitigating Social Media Risks

April 22, 2013

Yo Delmar,
MBA, CMC, CISM, CGEIT
Vice President, GRC Solutions
MetricStream

MetricStream

Social Media – Unavoidable?

Patients

- Share experiences, treatments they have gone through with fellow patients and providers
- A way to step-up the treatment and healing process

Providers

- Share experiences, treatments they have gone through with fellow providers
- Serves as an effective marketing tool
- Breaks the barrier of time and distance

MetricStream

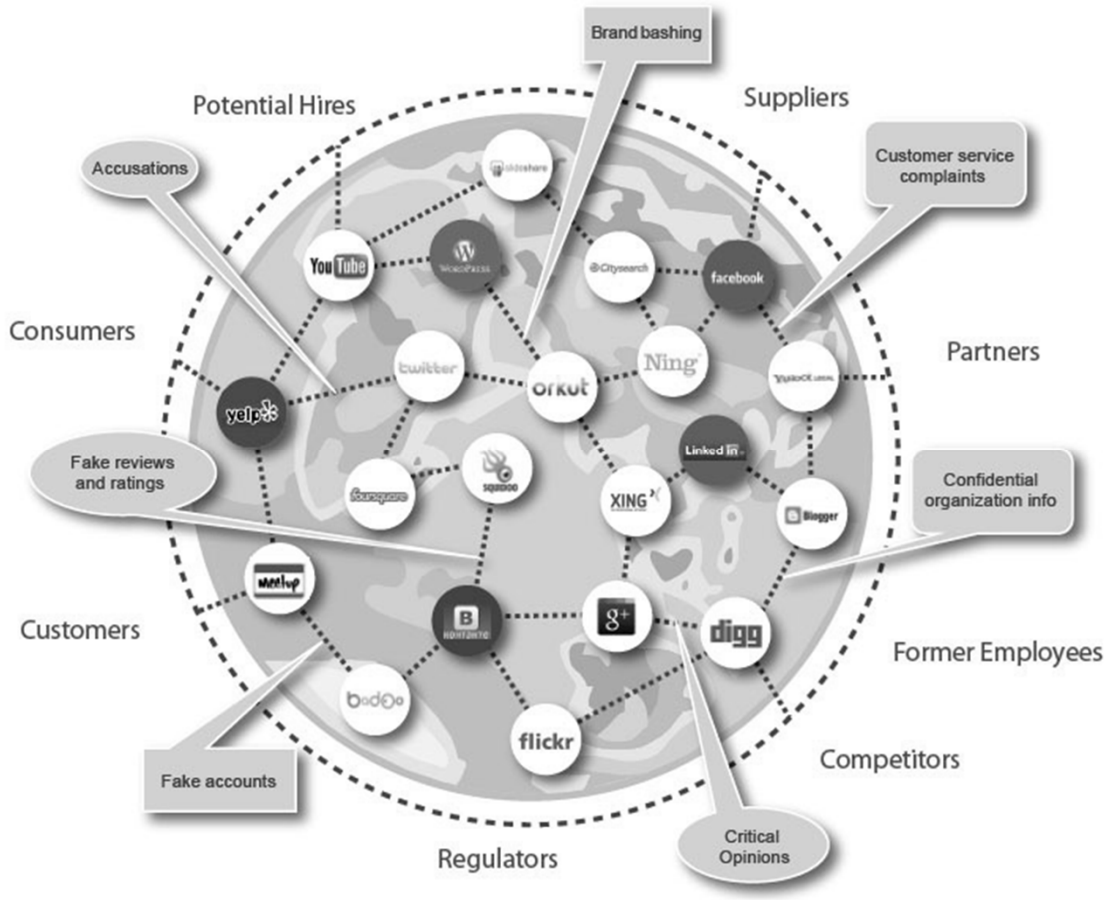
The Challenges Thrown…

- Power of One
    - One blog, one tweet, one post, one video, one photo, one incident
    - Impact and influence of one is dramatically high
    - Snowball effect - starts small, builds upon itself, becoming larger and perhaps potentially dangerous or disastrous
    - It is available anywhere and anytime
- You are Dealing with Big Data
    - Volume, Velocity, Variety
- Authenticity of Sources and Content
    - Difficult to verify
    - Matters less with low attention spans
- Blurs the lines between Professional and Personal Lives

…… It continues to evolve

MetricStream

Social Media: What Comes Along with Benefits?

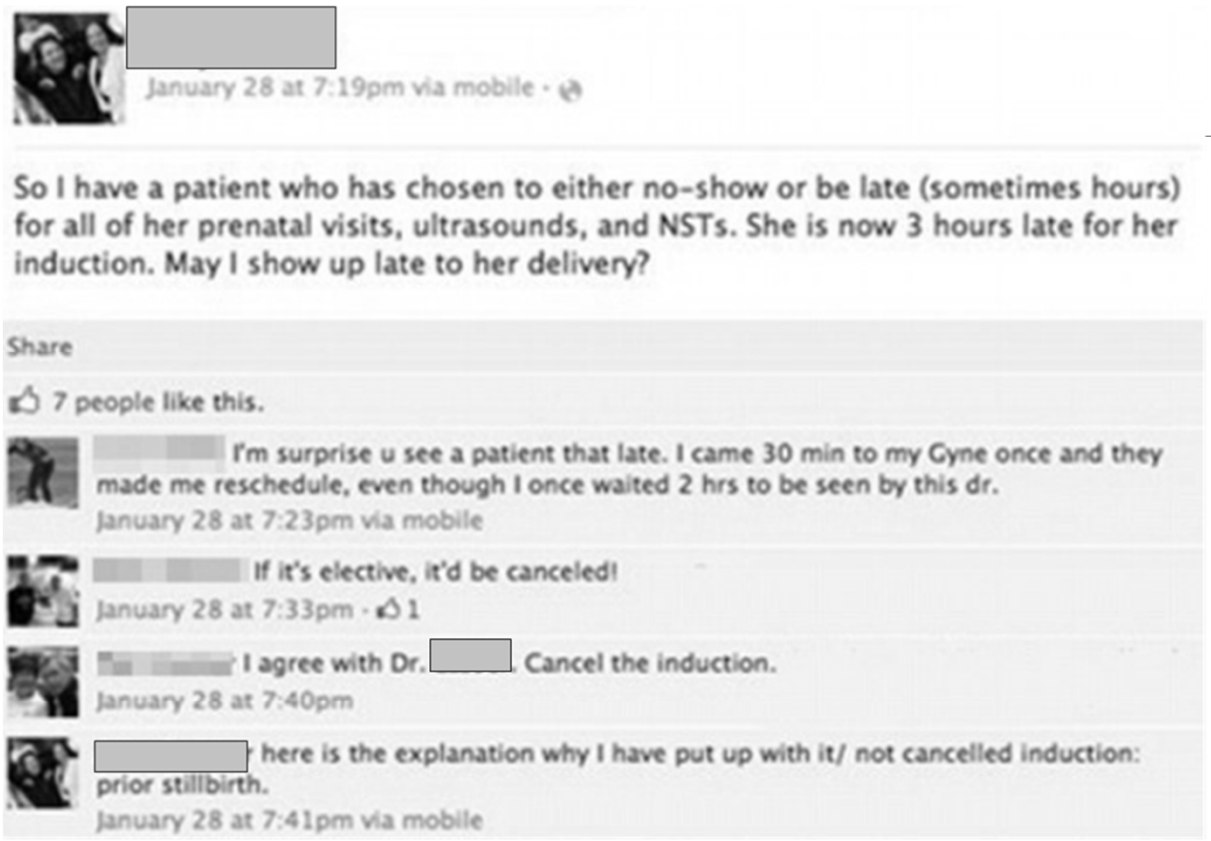


Brand and Reputation
Brand bashing
Fake reviews and ratings
False accusations
Customer service complaints
Fake user accounts
Loss of control

Regulatory and Compliance
BYOD culture
Privacy violations
Regulations
No industry standards
Lack of formal processes
Outdated strategies

Data Privacy & Security
Phishing
Account hijacking
Intellectual property loss
Confidential data exposure
Malware and spam

MetricStream



A Doctor posted her frustrations about a patient who was late for appointments onto Facebook and divulged her patient's history

Social Media Governance Program Components

Bottom-up Approach

Social Media Monitoring

Detection, Analysis, Mitigation, Control

Incident & Remediation Management

- Continuous monitoring for incident violations and implementing corrective and preventive measures to avoid re-occurrences

Top-Down Approach

Policy Management

- Developing, Implementing and Monitoring Policy adherence

Compliance Management

- Tracking changes in HIPAA regulations, measuring impact and aligning controls

Risk Management

- Assess and mitigate the risks of non compliance with HIPAA and magnitude of impact

Training Management

- Streamlining the training process from assigning training program to completion

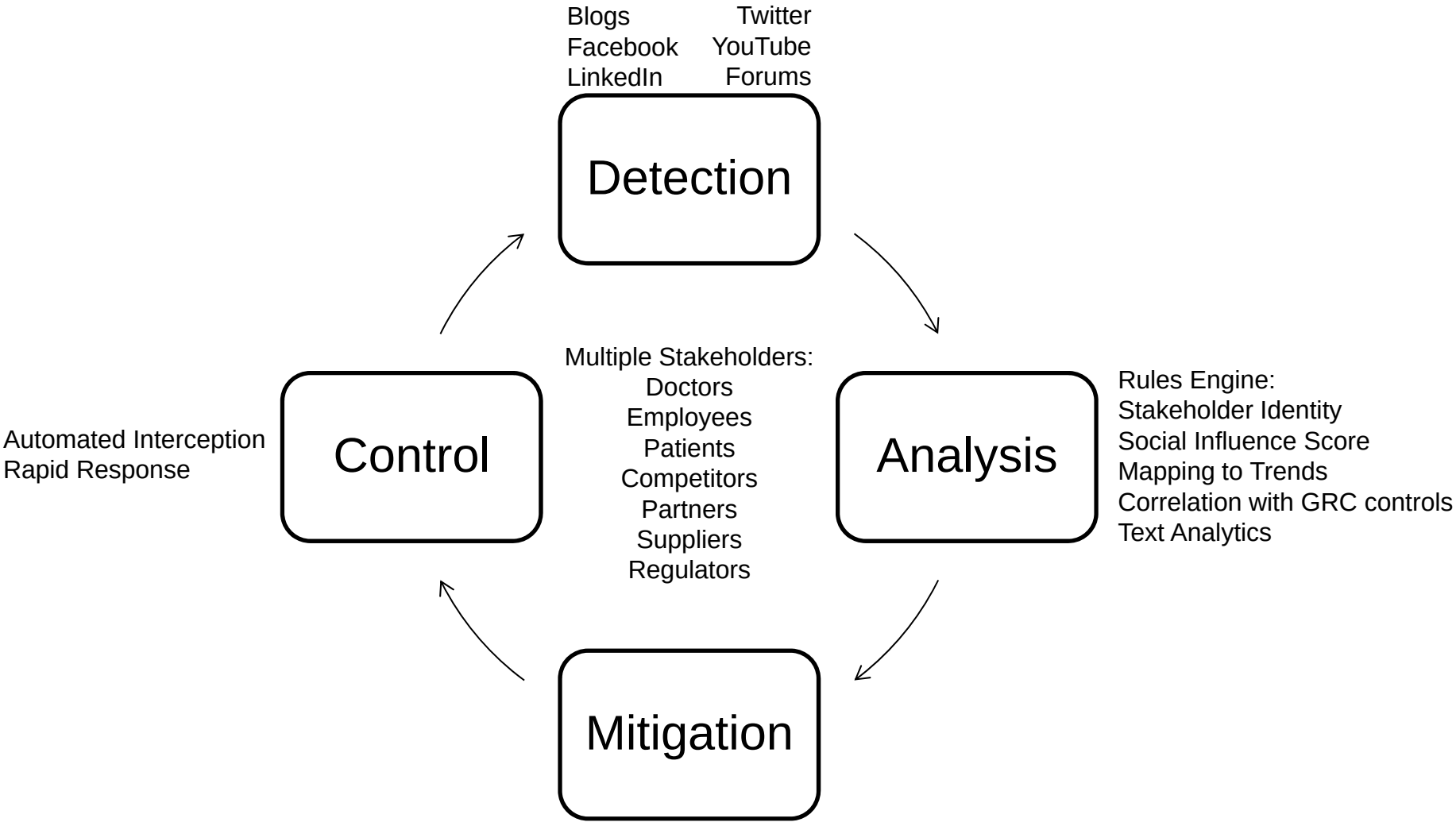
MetricStream

Top-Down Approach

- Start with risks to business objectives and goals
- Map to potential threats from social media
- Provide context to the risks within ERM framework
- Leverage bottom-up data effectively for mitigation

MetricStream

Effective Social Media Monitoring



MetricStream

Social Media Policies

- Be brief and to the point
- Cover Blogging, Social Networks, Collaborative Wikis
- Separation of Personal and Business activity
- Provide Examples of what to do and what not to do
- Say how you will manage any business presence
- Define Responsibilities for Official Representatives
- Define Rules for establishing any new presence on-line
- Provide for regular reviews of usage to stay within bounds of HIPAA privacy and security rules
- Training, training, training!!
- Documentation, documentation, documentation!!

MetricStream

HIPAA Driven Social Media Policy Management

- Define Social Media Policy modeling HIPAA elements
- Dovetail with employment policies
- Distinguish use of covered entity vs. personal technology
- Define Social Media forums/ blogs/ Vlogs
- Prohibit Disclosure of Confidential Information
- Provide Social Media relevant examples of PHI

Creation & Storage of Social Media Policy

- Ensure every aspect of PHI violations and HIPAA compliance are covered

Review & Approval of Policy

- Map all the policies to risks and controls for clear understanding
- Emphasizes on magnitude of impact in case of violation
- Outline protection in litigation

Mapping to Risks & Controls

- Keep organization aware of the policies
- Prevent improper use of Social Media

Awareness & Training

- Govern how employees use social media in and out of the workforce
- Provide enterprise wide visibility

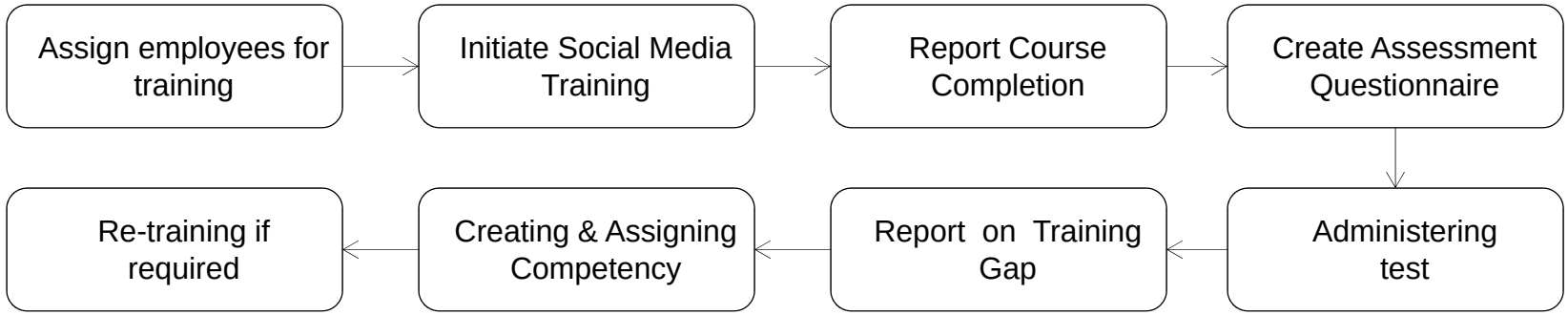
Tracking & Visibility

MetricStream

Training Management

A recent survey by the Society for Human Resource Management about social media in the workplace revealed that 73 percent of respondents said their organizations do not offer social media training for employees who use social media for business use.

- Employees must be trained to safely use social media and comply with HIPAA
- Social Media compliance challenges are due to lack of training
- Imparting training provides a forum for trainees to ask questions and receive quick responses
- Enables organizations to complement healthcare marketing efforts



MetricStream

Risk Management

Risk Scoping

- Process
- Hospital Entity
- Hospital Location

Library of Risks

- PHI disclosure terms
- Services/Work conditions
- Policy Gaps
- HIPAA violations

Risk Factors

- Provider-Patient in different locations
- Lack of Awareness of POLICIES and PROCEDURES

Risk Mitigation

Inherent Risks

Ranking of Risks

What-If Analysis

Risk Mitigation

Residual Risk

Controls

Internal Audit

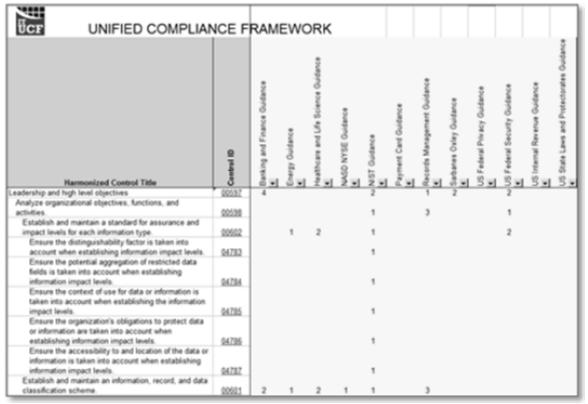
Internal Audit

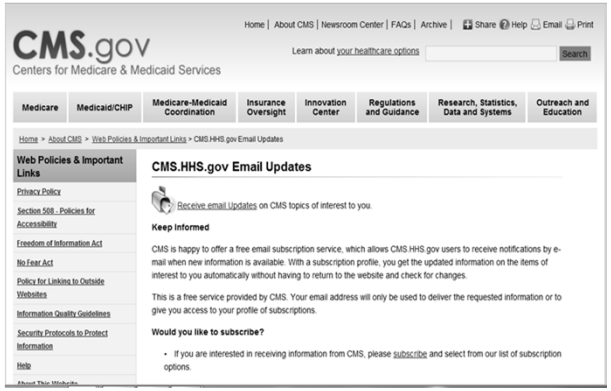
3rd Party Testing

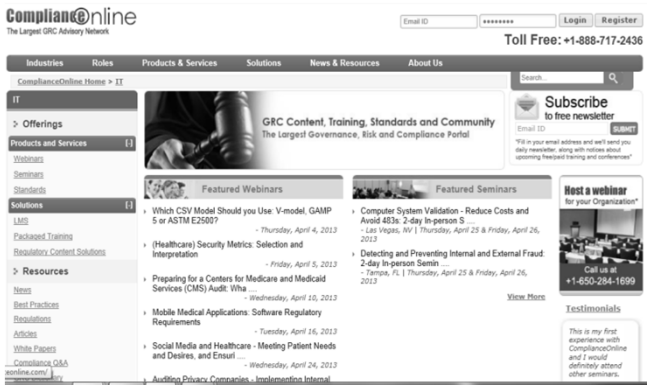
Compliance Strategy

MetricStream

Aligning to Regulatory Changes







Keep track of Changes in HIPAA/HITECH requirements

Align your Risk and Compliance Program

Carry out a Risk Assessment to understand the Impact

Ongoing Training Programs to keep the Employees updated

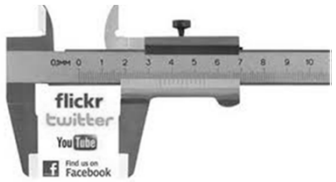
Keeping Your Policies & Procedures updated

Identify New Controls or Align Your existing controls

MetricStream

Metrics to Monitor

Social Media Compliance Program Sustenance Metrics



PREVENTIVE METRICS

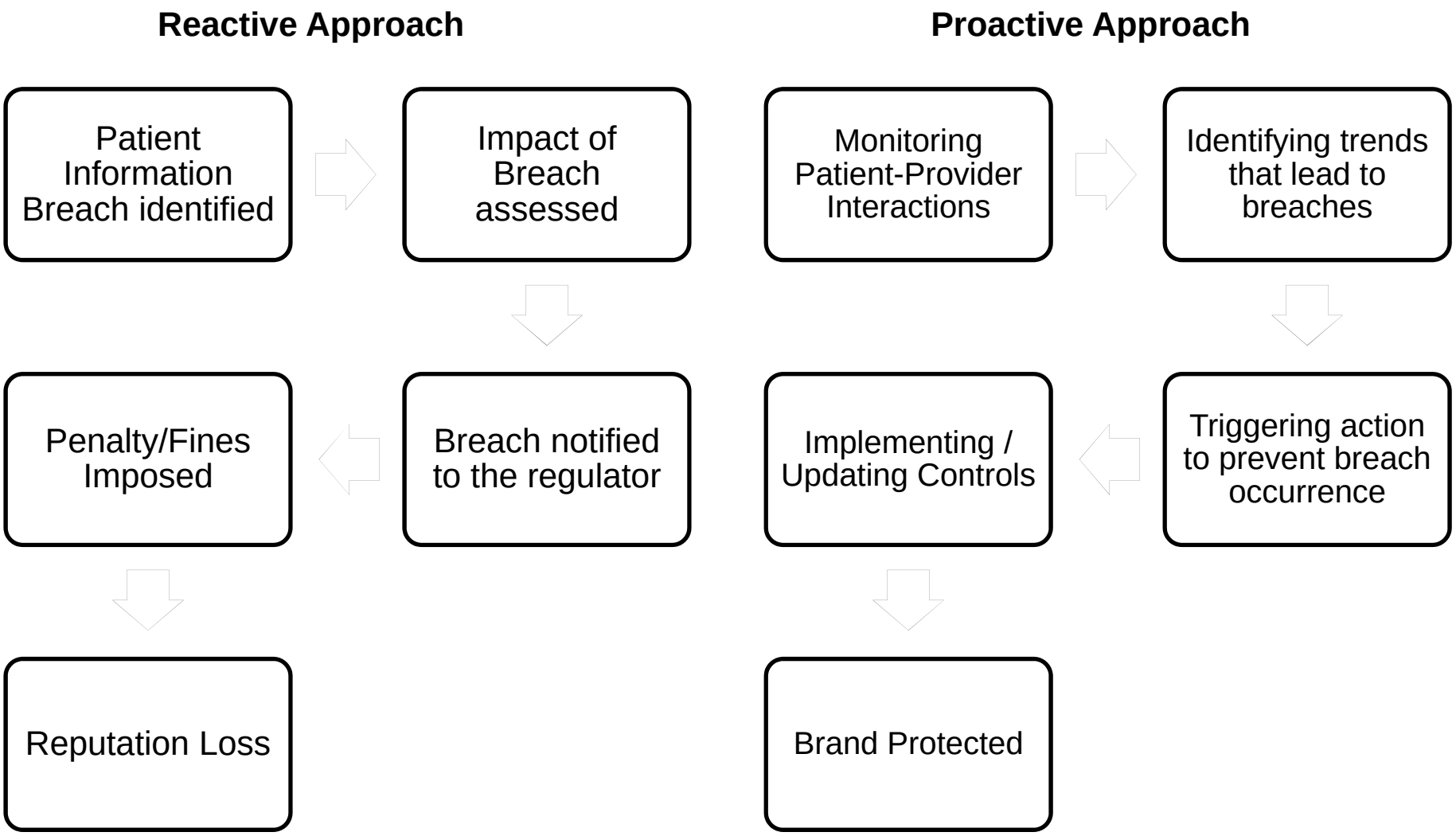
- Real-time view of the number of HIPAA violations
- Obsolescence of policies with changes in HIPAA regulations
- Employee usage of Social Media tools
- Frequency of Social Media Training imparted to the employees
- Gaps in the Training Program
- Information security risk assessment scores – Impact Vs Likelihood
- Number of threshold-limit breaches

CORRECTIVE METRICS

- Issues and findings identified from proactive compliance audits
- Sources of information security breaches and frequency
- Results of the remediation measures taken

MetricStream

Reactive Vs Proactive



MetricStream

Creating a Sustainable Governance Framework

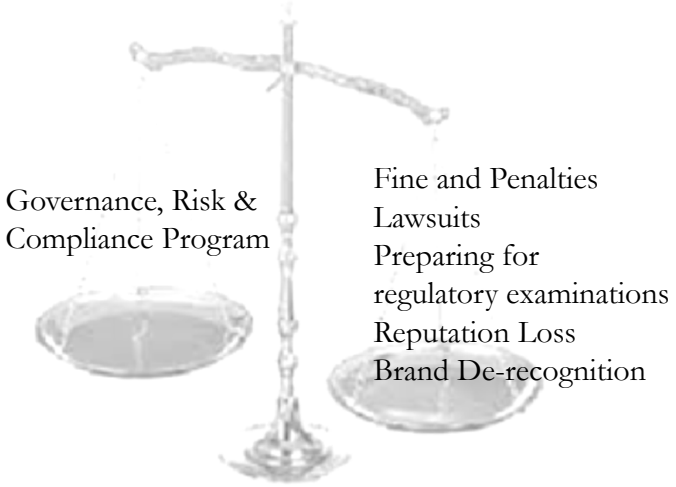
- Social Media Governance Integrated with GRC Program
  - Incorporate social media threats, risks and controls in enterprise GRC data model and risk and controls libraries
  - Address social media risks at a generic level
    - Not focusing on select websites or channels
  - Embed controls within day-to-day business processes
  - Include relevant social media risks in management reporting
  - Integrate with existing assurance programs
    - Internal controls, self assessments, security audits, internal audits, surveys, attestations, certifications

MetricStream

Business Case for A Governed Social Media Program

- "Profit = Sales – Cost of Operations" no longer holds good in today's complex ecosystem
- Profit = Sales - Cost of Operations – Notional Loss
- Cost of Operations will include
  - Reduced Stock Price
  - Fine and Penalties
  - Lawsuits
  - Preparing for regulatory examinations
  - …….
- Notional Loss will occur on account of
  - Reputation Loss
  - Brand de-recognition

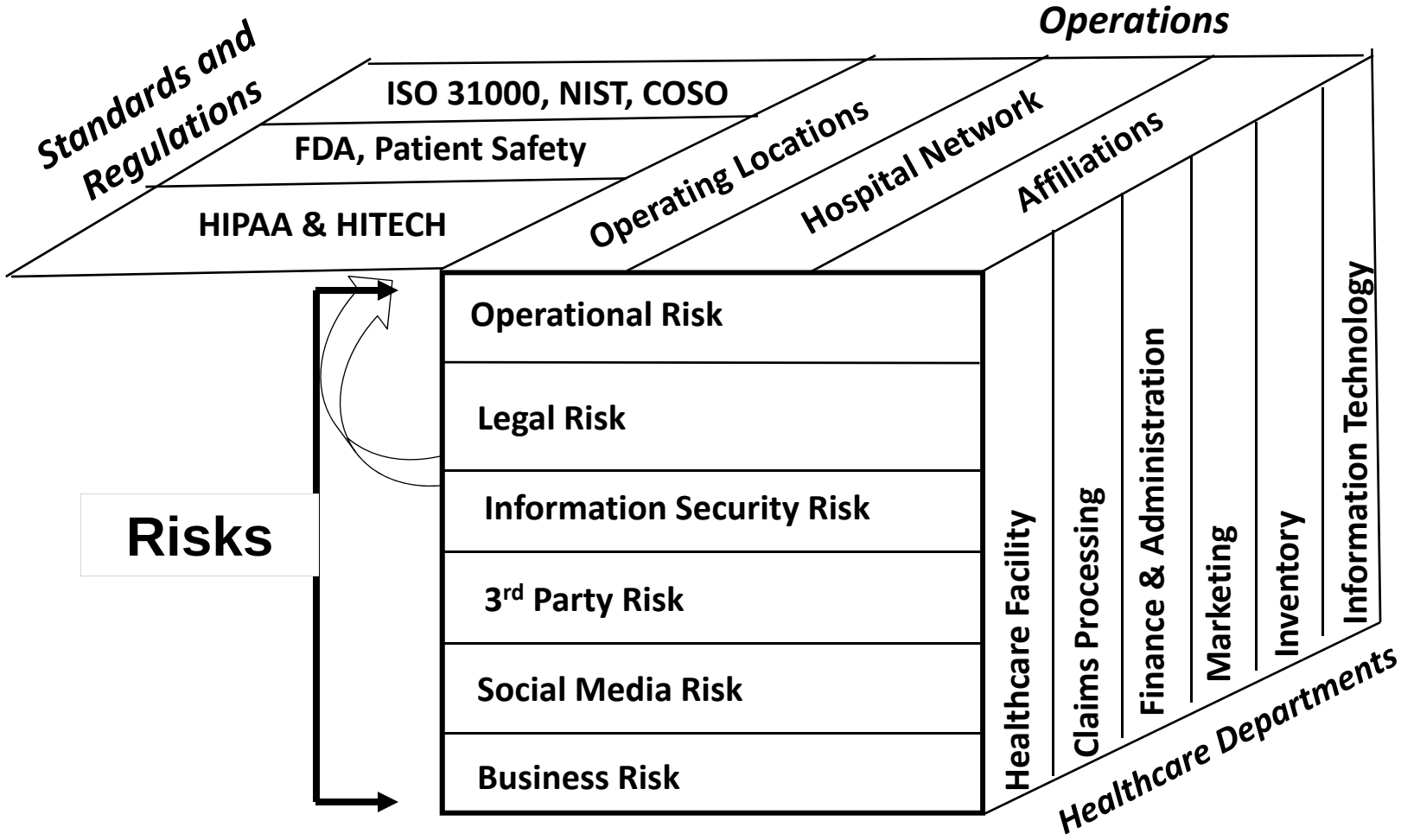
Cost of Operations & Notional Loss



MetricStream

The End Goal…

Centralized view of risk and compliance information for improved reputation and brand image



MetricStream

About MetricStream

Vision	Delivering Business Performance through Integrated Governance, Risk and Compliance
Applications	• Compliance Management • Risk Management • Internal Audit Management • Policy & Procedure Management • Issue and Incident Management • IT GRC • Supplier & Vendor Governance • Quality Management • Environmental Health & Safety • Energy & Sustainability Management
Market Leadership	• Serving Hundreds of Clients for Over 12 Years • Industry Specific GRC Offerings • Patented GRC Platform Technology
Analyst Recognition	FORRESTER® Leader in Forrester GRC Wave Gartner Leader in Gartner GRC Magic Quadrant
Contact us	• Website www.metricstream.com • Email info@metricstream.com • Phone +1-650-620-2955

MetricStream