Is Your Privacy Program Reactive or Proactive?

Tips and Tricks to Build a Proactive Program

Speaker Introductions

Jacki Monson
Sutter Health
Chief Privacy Officer
Office of the General Counsel

Jutta Williams
Intermountain Healthcare
Chief Privacy Officer
Business Ethics and Corporate Compliance
Objectives

– Identify the challenges and pitfalls for reactive privacy programs.
– Apply Compliance theory and the proactive approach to privacy; choosing a model that can anticipate and gracefully adapts to regulatory change.
– Explore practical experiences for building a proactive privacy program including quick wins will help leadership recognize your program’s value.

Reactive Privacy Program: Band Aid Approach

• Regulatory Risk
• Lack of Patient Trust
• Reputational Exposure
• Lack of Road Map and Prioritization
How is Privacy Organized?

Decentralized
- Policies are unique at each facility
- Teams develop goals and vision independently.
- Interpretation and application may vary.

Standardized
- Policies may differ but have minimum requirements.
- Education Objectives are coordinated.
- Interpretations are shared between teams.

Centralized
- Policies apply across all facilities
- Education is centrally assigned.
- All program activities are led by a central privacy team.

Tough Balancing Act

Maximize Opportunities to Innovate
- Create flexible processes
- Allow for uniqueness
- Adapt program to local cultures of caring

Keep Burdens and Liabilities Low
- Reduce response lags during times of change
- Reduce deviation from best practice
- Reduce duplication of effort
Fire Fighting vs. Fire Prevention

- Program responsibilities that are required to be HIPAA compliant.
- Opportunities to support other programs as a subject matter expert.
  - HIM, IT, Risk, Clinical Programs
- Some activities are inherently reactive “fire fights”.
  - i.e. investigation requests
- Some activities are proactive in nature and when done right act to prevent future fires.
  - i.e. privacy education

Where are your team’s efforts focused?
Is it balanced appropriately?

Proactive Program Tips and Tricks

Compliance Theory on Building Effective Programs

- Risk Assessment
- Oversight
- High Level Commitment
- Effective Lines of Communication
- Standards
- Policies & Procedures
- Training and Education
- Auditing and Monitoring
- Response and Prevention
- Enforcement and Discipline
- Designated Official
Named Privacy Official

- Each covered entity that exists in your system should have a named privacy official
- Create privacy champions across your organization to assist with privacy
- Ensure that privacy official develops relationships with all levels of the organization including:
  - Leadership
  - Front line staff
  - Key partners: Legal, HR, Risk Management

High Level Commitment

<table>
<thead>
<tr>
<th>Proactive Measures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a regular rather than ad-hoc meeting schedule</td>
</tr>
<tr>
<td>Deliver education to governance committees on privacy news – Especially recent enforcement activities, fines and penalties!</td>
</tr>
<tr>
<td>Develop Scorecards and send them as a matter of course</td>
</tr>
<tr>
<td>Ask leadership for advice; recognize their contribution to setting program strategy</td>
</tr>
<tr>
<td>Leverage the power of executive endorsement for program initiatives.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pitfalls to Avoid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not let them forget about you.</td>
</tr>
<tr>
<td>Do not make every meeting with your governance committee a bad news story</td>
</tr>
<tr>
<td>Typically, privacy programs identify risks and executives make decisions on risk appetite. Know who has decision rights in your organizations and engage them in discussions.</td>
</tr>
</tbody>
</table>
Program Oversight

- Chief Compliance Officer / Chief Risk Officer
- Privacy and Security Governance Committee
- Compliance Committee
- Audit and Compliance Committee of Board

Policies & Procedures

Proactive Measures
- Establish clear ownership for privacy policies.
- Review all policies on a routine basis.
- Invest in policy management and publication tools.
- Establish and/or adhere to policies on writing policies.
- Consistency is key

Pitfalls to Avoid
- **X** Policies without defined terms. E.g., what is a “treating relationship.”
- **X** Failing to update secondary materials
- **X** Writing policies that are too lengthy or to hard to understand
- **X** Forgetting that audits expect 100% compliance with policies.
- **X** If exceptions are expected, define a process.

Remember readability matters. Policies are not just regulatory requirements. Workforce wants to do the right thing - we need to make sure they can understand what that is.
Training & Education

— Privacy Education
  • Monthly newsletters
  • Annual training
  • Patient impact stories
  • Staff meetings
  • Role based training eg. Physician specific education

— Policy Attestations

— FAQ Database

Effective Lines of Communication

Proactive Measures
  ▶ Advertise information about privacy rights in public places.
    ▪ Is your NPP listed on your website’s privacy page or does it just a message from your webmaster about cookies?
  ▶ Widely advertise how to contact your office.
    ▪ Email address, phone number, mailing address

Pitfalls to Avoid
  ✗ Forgetting to advertise your communication channels.
  ✗ Fail to respond to privacy concerns – even if its just to confirm receipt of the communication.
  ✗ Requiring specific forms to request amendments, AOD or restrictions, but not making them available for download.

When was the last time that you looked at your company’s public website? Can a patient or concerned employee find you?
Auditing & Monitoring

- **Computerized**
  - Implement technology to assist
  - Focus on a 3-4 rules

- **Physical**
  - Create audit tool
  - Incorporate in Joint Commission tracers questions
  - Require high risk areas to submit self audits bi-monthly

Investigations & Discipline

**Proactive Measures**
- Work with HR to establish and educate to a formal discipline policy for privacy violations.
- Measure how investigations are going:
  - How long to closure?
  - How often is notice required?
  - Which facilities are doing well?
  - How often is a violation confirmed?
  - What types of incidents are trending?

**Pitfalls to Avoid**
- Inconsistent application of a discipline policy.
- Incomplete investigation notes. You never know when an OCR inquiry may come.
- Failing to document breach notification decision justifications in investigation notes.

*Don't Forget to celebrate successes! Write thank you cards to workforce when investigation reveals they did the right thing.*
Enforcement & Discipline

- Ensure consistent disciplinary process across organization
- Corrective action plans
- Consistent investigations
- Complete documentation

Response and Prevention

Proactive Measures
- Prepare for catastrophic breach before an incident.
  - Build an incident plan
  - Contract with a breach response vendor now.
- Stay involved in the legislative process at both state and federal levels.

Pitfalls to Avoid
- Figuring out your response plan after a large breach has already occurred.
- Failing to be involved in the planning phase for key initiatives that involve patient information.
- Doing nothing when you see proposed law that harms your organization.
## Risk Assessment

### Proactive Measures
- Assess the state of your program at least annually.
- Build a workplan for your team that addresses program gaps.
- Add time to your calendar to work on these goals.
- Think like an auditor:

### Pitfalls to Avoid
- **✗** Letting acute issues take over. If you knew about an issue and did nothing about it, it could become classified as reckless disregard.
- **✗** Failing to follow HIPAA guidelines for documenting addressable requirements.
- **✗** Forgetting to document why something was considered “reasonable and appropriate” during a risk assessment.

## Reporting

- Scorecard
- Risk dashboard
- Metrics that are measurable over time
- Identify opportunities through trending privacy incidents
- Regular reporting to leadership
Response & Prevention

- Privacy By Design
- Develop processes to proactively address high risks
- Conduct annual risk assessment
- Incident response plan- practice it
- Root cause analysis
- Mock audits

Closing Thoughts

- Reporting metrics crucial to measurable value for resource request
- Create a program that works for your organization, it’s not a one size fits all approach
- Developing key relationships with your leadership is key to your success
Contact Information

Jutta Williams
Chief Privacy Officer
Intermountain Healthcare
Jutta.Williams@imail.org

Jacki Monson
Chief Privacy Officer
Sutter Health
Email: monsonja@sutterhealth.org