Evaluating Privacy Compliance Program Effectiveness

HCCA Compliance Institute
April 27-30, 2003

Brian S. Felton
Why Measure Privacy Compliance Program Effectiveness?

- Measurement can lead to more **disciplined goal-setting** regarding privacy compliance.
- Measurement can help to **focus limited resources**.
- Measurement can help to **enhance accountability** and help create a **culture of compliance**.
- Measurement can provide data to **inform decision-makers** and **drive change**.
- Measurement can **demonstrate due diligence** and **provide evidence of intent** to comply.
What is Effectiveness All About?

An effort is “effective” when it meets, to an acceptable degree, an established goal. In other words, the effort brings about the desired effect.

E.g., a cold medicine is effective if it reduces symptoms as expected – it need not cure the cold.

E.g., a leader is effective when he or she accomplishes organizational priorities – even if some tasks remain undone.
So to measure effectiveness, you must know:

- What results you wish to achieve. In other words, *what are your goals*?
- Whether, or how well, you achieved those results. In other words, *did you meet your goals, or how close did you come?*
Possible Privacy Compliance Program Goals

- Avoid civil, administrative and criminal penalties
- Deter violations of privacy obligations
- Minimize risk of private lawsuits
- Bolster/sustain public trust
- Enhance employee performance, loyalty and morale
- Reduce costs associated with stakeholder inquiries
- Support quality improvement
- Others
Measurement Models

**Single-Measure Model**: Measure along the most important dimension to bring clarity and focus (e.g., pole vault)

**Multiple-Measure Model**: Measure along multiple dimensions to see the big picture and address varying expectations (e.g., figure skating)
Single v. Multiple Measures

Single-measure approaches have appeal because they are easy to understand and apply.

May be appropriate when cost of ignoring other standards is low – such as when the single dimension is highly objective or where controls address other concerns.

E.g., we measure a hockey team’s success by the score at the end of the game – but we can address unsportsmanlike conduct through penalties that may indirectly affect a team’s score.
Multiple measures allow us to acknowledge different, even competing, considerations.

Can work when cost of measuring one dimension is unacceptably high – e.g., that standard is subjective, untested, or simply doesn’t tell the whole story.

E.g., an architectural student may receive a poor grade although a model is structurally sound, if the layout is impractical or the design aesthetically weak.
To evaluate privacy program effectiveness, use multiple measures at once. Why?

- Privacy rules are untested.
  - Some assumptions will be corrected
  - Some interpretations will be flawed
  - Some ambiguities will be clarified

- Where rules are untested, outcomes-only measurement risks scores that are skewed (negatively or positively).

- Example: Breach notification as mitigation of harm. Do we know what the standard really is?
Single v. Multiple Measures

To evaluate privacy program effectiveness, use multiple measures at once. Why?

- **Stakeholder needs vary.**
  - HIPAA mandates structural elements
  - Regulators look for due diligence
  - Customers expect right outcomes

- If you can show you did better than average, you are only part way there.

- Example: Zero privacy complaints documented. Is this good or bad?
To evaluate privacy program effectiveness, use multiple measures at once. Why?

– *More opportunities for improvement.*

Evaluating processes (not just outcomes) can correct potential or emerging issues sooner and at lower cost.

– Example: A periodic review of HIM training quality may prompt a change in authorization processes that reduces the risk of unauthorized disclosures before a complaint is even received.
Structure, Process, Outcomes Model

**Structure**: Are program components in place that increase the likelihood of compliance with privacy obligations?

**Process**: Do processes exist, and are processes followed, that increase the likelihood of compliance with privacy obligations?

**Outcomes**: Is the organization actually performing in accordance with identified privacy obligations?
Structure: Evaluating the Foundation

Privacy compliance program structure evaluation considers *components*, such as:

- Existence of written privacy standards (policies/procedures)
- Existence of compliance committee
- Presence of an independent compliance officer for privacy
- Availability of confidential reporting of privacy compliance concerns (e.g., hotline)
- Existence of compliance training materials and means for delivery of training
Process: Assessing the Work

Privacy compliance program process evaluation considers activities, such as:

– Efforts at communicating privacy policies and procedures
– Efforts at conforming to privacy policies and procedures
– Ongoing privacy awareness efforts
– Monitoring and auditing efforts
– Efforts to implement corrective action plans
Outcomes: Tracking the Results

Privacy compliance program outcomes evaluation considers results, such as:

- Number of reported violations of privacy policies/procedures
- Number of third-party complaints on privacy issues
- Number of disciplinary actions taken
- Response time for requests for access, amendment, accounting, etc.
- Percentage of records with accurate/complete documentation (e.g., required authorizations, NPP acknowledgement, accounting log, etc.)
Putting it All Together

1. Articulate general privacy compliance objectives

2. Articulate specific expectations for privacy program structure, processes and outcomes:
   – Map the expected structure
   – Describe expected processes
   – Delineate expected outcomes

3. Measure each at the level where measurement is most likely to effect change
4. Communicate findings and seek response, criticism, suggestions or assent

5. Develop, communicate and implement plans for addressing substandard measures, and track progress against the plans

6. Periodically communicate with senior management about compliance scores across the organization

7. Periodically revisit general privacy compliance objectives and specific SPO expectations
## Privacy Compliance Program Effectiveness
### Structure Measures

<table>
<thead>
<tr>
<th>Measure</th>
<th>Priority (H, M, L)</th>
<th>Criteria</th>
<th>Score (0 - 100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Policies and Procedures</td>
<td>Developed Approved Published Understandable Accessible to all staff Up-to-date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Committee</td>
<td>Constituted Appropriate membership Regular attendance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Officer</td>
<td>Designated/staffed Appropriate level in organization Appropriate reporting relationships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hotline</td>
<td>Established Publicized Independent 7 x 24 staffing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Materials</td>
<td>Developed Appropriate scope Understandable Up-to-date Accessible to all staff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disciplinary Mechanism</td>
<td>Established and documented Clear and consistent Communicated to relevant managers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguards</td>
<td>Safeguard needs have been assessed Reas. safeguards have been determined Safeguards decisions have been communicated Safeguard changes have been implemented Decisions regarding safeguards are documented</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designations</td>
<td>Organizational designations are made (ACE, contact person, etc.) and documented</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Privacy Compliance Program Effectiveness
### Process Measures

<table>
<thead>
<tr>
<th>Measure</th>
<th>Priority (H, M, L)</th>
<th>Criteria</th>
<th>Score (0 - 100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Education</td>
<td>Policies are communicated</td>
<td>Processes have been identified to promote ongoing privacy awareness</td>
<td></td>
</tr>
<tr>
<td>Processes</td>
<td>Staff has opportunity to raise questions</td>
<td>Processes are implemented</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Education is appropriate to staff background and responsibilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processes are followed for providing updated education as necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Awareness</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring and</td>
<td>Monitoring and auditing processes are developed and communicated</td>
<td>Disciplinary processes are developed, documented and communicated</td>
<td></td>
</tr>
<tr>
<td>Auditing Processes</td>
<td>Processes are implemented</td>
<td>Processes are implemented</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processes are viewed as collaborative efforts to improve</td>
<td>Disciplinary actions are appropriately documented</td>
<td></td>
</tr>
<tr>
<td>Disciplinary Processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corrective Action</td>
<td>Processes relating to corrective action plans are developed, documented and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processes</td>
<td>communicated</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processes are implemented</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff report progress against corrective action plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measure</td>
<td>Priority (H, M, L)</td>
<td>Criteria</td>
<td>Score (0 - 100)</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Third Party Complaints</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hotline Call Response/Resolution Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disciplinary Actions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Request Response Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amendment Request Response Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounting Request Response Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPP Acknowledgment Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounting Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrictions Request Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Contracts Signed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Measure the Measure

Does the measurement process provoke discussion, discomfort or disagreement?

Does the measurement process enhance the organization’s culture of privacy compliance?

Are the failures to meet objectives the result of poor performance or unrealistic expectations?
Measure the Measure

Is the measurement process surfacing the kinds of issues that worry people on the front lines?

Is the measurement process bringing people in the organization together or driving them apart?

Does the measurement process promote accountability but still encourage honest evaluation?
Privacy compliance programs pose unique measurement challenges:

• Baselines have not yet emerged. What level of performance merits green, yellow or red?

• Interplay of processes and outcomes. If HIPAA speaks to the “how,” is the “how” a process or an outcome?

• Numerical outcomes measures may not reflect relative risk.