P4: Designing an Effective Privacy Program

David Behinfar, Chief Privacy Officer
University of North Carolina Health

Adam Greene, Partner
Davis Wright Tremaine LLP

Katherine Georger, Associate Compliance Officer
Duke University Health System

Christopher Terrell, Deputy Chief Compliance Officer & Privacy Officer
Encompass Health

David J Behinfar, JD, LLM, CHC, CHRC, CCEP, HCISPP CIPP/US
Katherine Georger, JD, CHC, CHRC, CIPP/US

Duke University Health System is a world-class private, not-for-profit health care network dedicated to providing outstanding patient care, educating tomorrow's health care leaders, and discovering new and better ways to treat disease through clinical and biomedical research.

Founded in 1998 to provide efficient, responsive care, the health system offers a full network of health services and encompasses three highly regarded hospitals - Duke University Hospital, Durham Regional Hospital and Duke Raleigh Hospital - physician practices, home hospice care and various support services at locations across North Carolina.

Christopher Terrell, JD, CHC, CHPC

With a national footprint that spans 127 hospitals and 237 home health & hospice locations in 36 states and Puerto Rico, Encompass Health (NYSE: EHC) offers both facility-based and home-based patient care through its network of inpatient rehabilitation hospitals, home health agencies and hospice agencies.
Adam Greene, JD, MPH

Adam Greene, Partner
Davis, Wright, Tremaine, LLP

Adam is a nationally-recognized authority on HIPAA and the HITECH Act, primarily counsels health care systems and technology companies on compliance with the HIPAA privacy, security, and breach notification requirements.

A former regulator at the U.S. Department of Health and Human Services (HHS), Adam played a key role in administering and enforcing the HIPAA rules. At HHS, Adam was responsible for determining how HIPAA rules apply to new and emerging health information technologies and he was instrumental in the development of the current enforcement process.

Time For A Promotion

After your hospital merged with a regional health system, you have been promoted from privacy officer of a small critical access hospital, to the chief privacy officer of a regional health system with 25,000 employees.
Congratulations!

Our Deepest Condolences
Welcome To Regional Health System . . .

One problem ... the regional health system did not previously designate a full-time privacy officer. Or the person who was there did nothing to build an actual privacy compliance program. His/her motto was: “it’s all good”

SHAKA BRAH!

Where Do You Start?
Where Do You Start?

1. Perform GAP Analysis.
2. Develop relationships with internal partners (general counsel, information security, procurement, risk management, others...).
3. Assess Culture.
4. Check your 401(k) and consider early retirement.

Evaluating Presence Of Program Fundamentals

GAP Analysis

➢ Where are you now?
➢ Where do you want to be?
GAP Analysis

Great idea – we’ll take six months to prepare a full analysis of the program! Maybe we can hire a vendor to do this...

Advice From The Front Lines: Use The “Effective Elements Of A Compliance Program” To Quickly Perform A GAP Analysis

How Do I Do That Exactly?

**Answer:** Let’s do a quick recap of the US Sentencing Guidelines – and the Seven Effective Elements of a Compliance Plan.
What Happens When A Health Care Organization Breaks The Law?

The four factors that increase the ultimate punishment of an organization are: (i) the involvement in or tolerance of criminal activity; (ii) the prior history of the organization; (iii) the violation of an order; and (iv) the obstruction of justice.

The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility.

Reducing/Avoiding Penalties Through Proactive Measures

• These guidelines offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program.
• The prevention and detection of criminal conduct, as facilitated by an effective compliance and ethics program, will assist an organization in encouraging ethical conduct and in complying fully with all applicable laws.


What Is An Effective Compliance Program?

Seven Elements of an Effective Compliance Program:
1. Hire a professional to lead compliance efforts
2. Policies
3. Training
4. Auditing and Monitoring for Compliance
5. Incident reporting & non-retaliation / whistleblower protections (Compliance Hotline)
6. Investigations (with whistleblower protections)
7. Sanctions / discipline for noncompliance
Here’s What A High-Level GAP Analysis Might Look Like

<table>
<thead>
<tr>
<th>Evaluation Element</th>
<th>Good</th>
<th>Better</th>
<th>Best</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professionals /Staff</td>
<td>I am an office of one</td>
<td>We have staff</td>
<td>We are fully staffed</td>
</tr>
<tr>
<td>Policies</td>
<td>We have HIPAA policies</td>
<td>They are written, available to all staff and up to date</td>
<td>We also have a crosswalk with the Privacy Rule</td>
</tr>
<tr>
<td>Audits</td>
<td>I manually audit EHR access monthly</td>
<td>We have a tool that automates EHR access audits</td>
<td>We have a tool and staff who audit EHR access</td>
</tr>
<tr>
<td>Training</td>
<td>HIPAA training is offered annually and at NEO</td>
<td>We also educate as needed - all documented</td>
<td>We have a formal training plan in place</td>
</tr>
<tr>
<td>Incident Reporting/Non-Retaliation</td>
<td>We have a phone number and office email to receive reports</td>
<td>We have an intake method for anonymous concerns</td>
<td>We have an anonymous phone line and web-based portal for reporting</td>
</tr>
<tr>
<td>Incident Investigation</td>
<td>We investigate incidents</td>
<td>We have solid documentation</td>
<td>We have solid metrics and an application</td>
</tr>
<tr>
<td>Corrective Actions</td>
<td>People are disciplined for violations</td>
<td>People get fired (we take this stuff seriously)</td>
<td>Staff and Physicians understand consequences</td>
</tr>
</tbody>
</table>

After The GAP Analysis Is Complete

What Should I Do Next?
Evaluate The Intangibles

Regulatory requirements have been addressed... but there’s often much more to consider in building a privacy compliance program.

Assess Institutional Support For Privacy

Does your leadership truly support the mission of your office?

- Funding
- Presence at leadership meetings
- Are you brought in as a valued/trusted advisor?
- Do you report on metrics to leadership (not just to your compliance committee)?
Identify Your Strategic Partners

- Compliance
- Legal
- Procurement/Contracts
- Risk Management
- Information Security
- Medical / Administrative Departments
- Physicians
- Members of Administration
- Outside Counsel

Appreciate Your Organizational Culture

Just like people, institutions have their individual identities that shape risk tolerance and impact organizational decision-making.

How would you describe your institution?

- Serious
- Risk-taker
- Easy going
- Profit-focused
Recognize Institutional Politics

Do you know who at your institution will stab you in the back and throw you under the bus and then feed you to the dogs to dispose of your body?

Recognize Institutional Politics (cont.)

And do you know who will try and protect you and perhaps save you?
Understand Common Challenges

Is there a powerful force that is preventing the good that you are trying to do?

*Privacy, I am your general counsel*

Dori and Nemo are in the Privacy Office

Is Cultural Sophistication An Issue?

Does the following represent the complete understanding of HIPAA Privacy at your institution?

Shhhhh!

*UH OH. SOMEONE JUST COMMITTED A HIPPO VIOLATION*
Assessment To Action

Wow figuring out the status of the program, institutional support (resources available), the political environment, the cultural sophistication and who out there will support our office was a lot of work!

What’s Next?

**Answer:** Now you actually have to start doing something.

Phase 1 – Let’s Talk Budget

The budget cycle is rolling around.
- How many FTEs do you request?
- What will be their roles?
- What tools/applications will you request?
- How about professional conferences?
- How will you justify your requests?
You Already Did The Work…

- Performing a GAP Analysis (even if it is a make-shift analysis you just made up on the fly) can come in handy now.
- Presenting the “here’s the things we are supposed to be doing, but we are not – or we are doing them but not well” requests...
- Leveraging examples of settlements and financial penalties to reinforce your point.

Phase 2 – Things Are Finally Getting Done!

Policies and procedures are in place and 95% of the workforce is documented as having received their HIPAA training last year.

Where Should Your Focus Shift To Next?
How Your Current Program & GAP Analysis Can Continue To Drive Your Focus

- You know whether there may be funds for something like an electronic access audit tool or an incident management tool. If so, this may be where you go next.
- Or, you may need to improve training . . .
- Has OCR been making noise lately?
- The point is your attention and direction should be dictated by your vision and the results of your institutional resources and support as well as your evaluation of risk.

Remember – When Requesting Resources … Persistence Is Key

Persistence

"In the confrontation between the stream and the rock, the stream always wins; not through strength, but through persistence."

~Buddha
Phase 3 – The Dreaded Breach

At the end of February, you reported a breach (via the web - under 500) involving a workforce member misdirecting a secure e-mail containing a spreadsheet with 372 names, SS#s, sensitive diagnosis. . .

You just received a letter from OCR initiating an investigation and including a document request.

The OCR Investigation

➢ You would like to prepare a simple straight-forward response to the OCR inquiry.

➢ General counsel would like to send a 12-volume 5,000 page response to OCR.

➢ Litigate or Cooperate? What’s the best strategy?
The OCR Investigation (cont.)

You created a new policy after the breach requiring employees to double-check e-mail addresses. OCR did not ask for it. Do you produce it anyway?

1. Yes
2. No

Tips On Working With OCR

- Be professional
- Be respectful
- Be honest
- It’s OK to advocate for your organization
- Hire outside counsel/consultants if internal expertise/experience is lacking (computer forensics is one example)
Establishing An Incident Management Process

- HIPAA / HITECH Breach Risk Assessment
  - Who makes the call? (there is ALWAYS some subjectivity here)
  - Who drives the notification process?
  - Do you have vendors lined up for
    - the mailing
    - the call center
    - credit monitoring

Phase 4 – Things Are in Full Swing – Now It’s Time For Metrics

Evaluating your program and building metrics

1. What are you actually doing on a day-to-day basis?
2. And how are you improving the institutional program?

Building metrics helps keeps you on track and better ties your program to overarching organizational objectives.
### Training Metrics

**Do you have a Training Plan that will permit more than simple metrics?**

- In person training: Executive, NEO, Annual (all staff), specialized
- Electronic training: NEO, Annual (all staff), specialized
- Training offered at staff or leadership meetings
- In-service education (lunch and learn)
- Homegrown and outsourced training
- Newsletters
- White papers, infographics
- Training offered after incidents occur
- Do you have a library of training resources

### Auditing Metrics

**Routine audits validating your organization’s compliance with Privacy Rule provisions – some examples:**

- EHR access audits
- NPP offered at first visit and Acknowledgement signed
- BAAs in place – using current form

**Metrics on:**

- Audit type
- Entity level
- Disciplinary action for audits indicating violations
- Corrective actions and report results
Consult And Guidance Metrics

Here is one example for collecting and recording this data

<table>
<thead>
<tr>
<th>Consult</th>
<th>Consult Request Date</th>
<th>Assigned To</th>
<th>Requester’s Title, Dept &amp; Contact Person and/or Area</th>
<th>Nature of PO Consult &amp; Self Investigation</th>
<th>Type of Consult</th>
<th>Type of Data</th>
<th>Source of Request</th>
<th>Method of Response</th>
<th>Status</th>
<th>Close Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1003</td>
<td>6/2/2017</td>
<td>DB</td>
<td>Pal Smith - UP Operations</td>
<td>Vendor cost revisions to copying files</td>
<td>UNCHC Staff</td>
<td>Phl</td>
<td>Phone (direct)</td>
<td>Phone</td>
<td>Closed</td>
<td></td>
<td>Concerns over releasing identifiable data. DB concerns over releasing PO to community physicians but have no treatment of what patients, PO to develop guidelines.</td>
</tr>
<tr>
<td>1004</td>
<td>5/1/2017</td>
<td>DB</td>
<td>L. Sardell, G. Gadis, A. Caucasian</td>
<td>Requests for access to claims data. Concerns over releasing identifiable data.</td>
<td>UNCHC Staff</td>
<td>Phl</td>
<td>Email (direct)</td>
<td>Phone</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>8/15/2017</td>
<td>DB</td>
<td>Fee Molder, Clio Mgr</td>
<td>Concerns over Fully providing PO for Smoking-MAR as BAA</td>
<td>UNCHC Staff</td>
<td>Phl</td>
<td>Email (direct)</td>
<td>Phone</td>
<td>Closed</td>
<td>6/10/2016</td>
<td>DB shared details on data sharing with F. Molder with legal. Decision to permit release of existing data elements.</td>
</tr>
</tbody>
</table>

Program Metrics (KPIs) – At A Glance

Key Privacy Office Performance Indicators

<table>
<thead>
<tr>
<th>Monitoring Area</th>
<th>Privacy Services Key Performance Indicators</th>
<th>Goal</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Office Projects</td>
<td>Complete Privacy Projects / Internal Initiatives</td>
<td>≥55%</td>
<td></td>
</tr>
<tr>
<td>Access Auditing</td>
<td>Epic User Access Audits (monthly)</td>
<td>≥75%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Focused Audits</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Privacy Investigations</td>
<td>Complete all Privacy Investigations in advance of regulatory deadlines</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Consultations and Advisory Services</td>
<td>Respond to Requests for Consultations and Provide Advisory Services</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Most regulatory requirements for completion of substantiated investigations of incidents involving 500+ affected individuals, including provision of notice of affected individuals, the Office for Civil Rights and the Office of the NC Attorney General, as applicable</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>High Risk Incident Investigation and Breach Notification</td>
<td>Policies Developed, Reviewed, Revised and/or Replaced</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policies and Procedures Standardized Access Systems</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>Revisit/Update System on-line HIPAA Training</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Education and Outreach</td>
<td>Coordination of Privacy Functions with Network Entities</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct In-Service and Staff Education</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>
Open Discussion/Questions