Compliance, Privacy and Security Program Assessments Best Practice

Bret S. Bissey, MBA, FACHE, CHC
Vice President, Chief Compliance Officer, Gateway Health

Kelly McLendon, RHIA, CHPS
Managing Director, CompliancePro Solutions

Agenda

1. Introduction
2. Compliance Program Review
3. Privacy and Security Assessments
4. Cybersecurity has Arisen and Privacy is Rising
5. Best Practice Privacy and Security Assessment Examples
6. Q&A
Bret S. Bissey, MBA, FACHE, CHC, CMPE  
Vice President, Chief Compliance Officer at Gateway Health

- 30 years of diversified healthcare management, operations and compliance experience
- Former SVP, chief of ethics and compliance officer at UMDNJ
  - Credited with re-engineering the compliance program of the nation’s largest free-standing public health sciences university
  - Successfully led the compliance program to adhere to CIA with DHHS/OIG that occurred following a Deferred Prosecution Agreement
- Chief Compliance and Privacy officer at Deborah Heart and Lung Center
  - Three-year CIA, first settlement of Voluntary Disclosure Protocol
  - Compliance program recognized by HCCA as a “Best Practice”
- Author of Compliance Officer’s Handbook

Kelly Mclendon, RHIA, CHPS  
Managing Director CompliancePro Solutions

- 40 Years of HIM, EHR, EDM and Privacy and Security Compliance Management
- Designs and Implements privacy and security software and content
- Author of numerous articles, webinars and varied compliance content
- Creator of a KLAS ranked #1 product line
- 2015 AHIMA Innovator Triumph Award
- 2008 FHIMA Distinguished Member Award
- 2003 AHIMA Visionary Award
- 1992 Winner of 2 AHIMA Literary Awards
- 1990 Published the first article on Optical Disk Imaging technology ever in the journal of the AMRA
Session Goals

- Ideas for conducting a compliance program review to ultimately reduce overall organizational compliance risk
- How to utilize the elements of the DHHS OIG Model Compliance Program(s) to develop a work plan to perform this assessment
- The content of and tips for performing HIPAA privacy and security assessments in order to impress OCR and other privacy and security regulators
- Facilitate a high level of compliance which ultimately reduces organizational risk

Evaluating Your Compliance Program
Applicable Government Guidance on Compliance Programs

- DHHS OIG Compliance Program Guidance for Hospitals
- DOJ Compliance Program Guidance on Evaluation of Corporate Compliance Programs (February, 2017)

Government Guidance – “Gold” Standard

- Original OIG Compliance Program Guidance for Hospitals:
  - “Effective” is referenced 19 times.
  - Means it is important.
  - OIG states it needs “benchmarking” compliance program progress but doesn’t provide much direction.
Surveys to Evaluate

- Compliance culture – attempt to measure covered persons’ attitudes and views regarding the organization’s commitment to compliance.
  - Is it real or a sham?
- Employee compliance knowledge.
- Goal – provide evidence of program effectiveness.
  - Your leadership and board should be asking for this… and….
  - Elements to include: employee surveys, management assessments, audit results vs. benchmark, investigation numerics, disciplinary numerics, trending overpayments, employee feedback….

Compliance Culture Survey

- Focus is on the beliefs and values of the organization’s members.
- Can all levels demonstrate commitment to compliance?
- Examples:
  - If an overpayment is needed to be refunded, is there any conflict in it occurring?
  - If a senior-level executive made an unethical or improper decision, would it be addressed?
  - If a major referring physician were involved in an unethical business practice, would your leadership make the proper decisions that are consistent with your compliance program?
Compliance Knowledge Survey

- Test knowledge of compliance program structure and operations.
- Who is the compliance officer?
- If you observed an unethical decision, illegal behavior, patient harm or violation of law or regulation, where would you report this incident(s)?
- Has your compliance message reached and resonated with your target audience?
- Both types of surveys allow you to benchmark and measure compliance effectiveness over time.
  - Goal is that survey trend shows better results....

DOJ Compliance Program Guidance on Evaluation of Corporate Compliance Programs (February 8, 2017)

- Not specific to health care industry
- But identifies elements which can be utilized in a evaluation of the compliance program
- Many elements similar to historical DHHS-OIG Guidance
- The guidance is presented in the form of compliance-focused questions that the DOJ Fraud Division might consider when evaluating a corporate compliance program; thus, good information to consider to utilize....
DOJ attention focused upon following elements:

- Analysis and Remediation of Underlying Misconduct
- Conduct of senior & middle management
- Stature of the compliance function
- Autonomy of the compliance function
- Compliance Program funding and resources
- Corporate response to expressed compliance concerns
- Process for responding to findings
- Disciplinary action consistency
- Risk Management Process
- Frequency of updates to policies and practices
- Direct reporting of compliance to Board

Elements to Consider in Your Evaluation Efforts
• Seven Elements of the OIG Model Compliance Program as an area to focus your evaluation (plus 2 other areas we will discuss later):

1. Compliance Officer & Program Oversight
2. Policies & Procedures
3. Education
4. Audit
5. Corrective Actions to Identified Problems
6. Open Communication
7. Enforce Violations

Fraud, Waste and Abuse

• Special Investigations Unit?
• Systems and Data Analytics?
• Policies?
• Education?
• Reporting Mechanisms?
• Corrective Actions?
• Referral of Cases?
• Investigation Process Timeliness?
FDR Oversight

- Required for Medicare Advantage Plans
- Good Idea for all plans to review
- Utilize the Model Compliance Plan 7 elements
- How are vendors and delegates being monitored?
- What documentation exists for these efforts?

Measurement of Compliance Performance

Define Expectation of Performance or Standard
Report Achievement
Measurement of Result – attention on variance

Example: Annual Compliance Education
Every Senior Leader (n=20) will receive 2 hours
16 achieved standard
Result – 75% achievement
Report reasons for variance and year to year comparison of results
Elements to Consider in Your Evaluation Efforts

- Hotline Calls.
- Education.
- Audit/Monitoring Results
- Potential Areas of Trending Your Coding, Billing Results.
- Audit Benchmarking Scorecard.
- Annual Audit Work Plan Completion.
- Budget Analytics.
- Other Data Points to Trend by Year.

Hotline Calls – Evaluation

- Do you include just calls or all matters “logged” by Compliance?
- Need to ensure you have a consistent measurement...
- How many of those matters resulted in:
  - Investigations?
  - Remediation?
  - Paybacks?
  - Disciplinary actions?
  - Other?
- Trending data is the key....
- What is your baseline?
- Deal with the compliance naysayers in your organization.
  - “This is only for HR matters”....
  - “it is a waste of time”
Education – Evaluation

• How much compliance education is enough?

• Follow DHHS OIG CIA requirement or establish your own expectations?
  o Have Board support.

• Establish standard for different groups – “I like the following:”
  o Staff except housekeeping and food service – 1 hour annually.
  o Executives – 2 hours annually.
  o Physicians – 2 hours annually.
  o Board – 2 hours annually.
  o *Exception – those involved in negotiating physician or referral arrangements 2 hours plus specific training on Stark and Anti-Kickback Statute by an expert...

• Can your organization tolerate this?
  o Answer will tell you about your compliance culture.

Board Education – Governance

• Tailor this to what is occurring (internally and externally).

• Risk (organization and personal).

• Compliance officer can communicate with the board whenever he or she wants without hesitation?

• Does CCO report to the board?

• Are board members involved in the compliance program oversight?

• What is the compliance knowledge level of the board?
  • Engage experts to assist in program functioning and validation of “effectiveness” of compliance program.
  • Can you get assistance (externally) when you deem necessary?

• Information flow from entity.
  • Is the board receiving all necessary information?
Chief Compliance Officer

Independence

• Can you make the proper decision without fear of some sort of retaliation?

• Examples:
  • The lead admitter of patients to your hospital is in violation of the medical records completion policy – can you revoke privileges as policy states?
  • The president’s spouse is asking to review sensitive and confidential information related to an upcoming community fundraiser. Can you treat her as if she were a normal citizen?

• Who validates this independence?

Chief Compliance Office

Knowledge/Experience

• The compliance officer should be a subject matter expert.
  • Certification to validate.
  • Conferences attended, presentations made to industry, etc...

• However, no one in this business knows everything.

• It is OK to say “I need help” – are you able to get help when you need it?
  • Example: coding and reimbursement issues...
Audit/Monitoring – Evaluation

• Looking for improvement.
• Be careful – creative people can make audit results look better than they are.
  - Must establish consistent measurements.
• Consider using Net Dollar Value Error Rate on consistent universe annually as one review.
  - 50 claim randomly selected probe sample – consistent with OIG requirements.
  - Five percent or below is an acceptable error rate...
  - Great way to have a consistent measurement year after year.
• Complement with other planned and focused reviews and trend the results.
• How many “for cause” reviews performed annually – comparison.

Audit Benchmarking Scorecard

<table>
<thead>
<tr>
<th></th>
<th>Net Dollar Value Error Rate yr 1</th>
<th>Net Dollar Value Error Rate yr 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANNUAL REVIEW</td>
<td>3.5%</td>
<td>5.2%</td>
</tr>
<tr>
<td>RISK AREA 1</td>
<td>10.9%</td>
<td>3.3%</td>
</tr>
<tr>
<td>RISK AREA 2</td>
<td>6.0%</td>
<td>4.5%</td>
</tr>
<tr>
<td>RISK AREA 3</td>
<td>2.1%</td>
<td>1.2%</td>
</tr>
</tbody>
</table>
Annual Audit Work Plan Completion

• Based upon approved annual work plan.
  o By Compliance/Audit Committee or Board.

• How many projects were on original plan?

• How many projects were added during year?

• How many were completed? Not completed?

• Trend to answer resources and accurate planning.

• If you are missing either bad budget or operational problem.

Budget Analytics

• Based upon operating and FTE budgets approved by Board or Compliance/Audit Committee.

• Operating budget variance ($$ and %).
  o Why a variance? Consultants?

• FTE budget variance ($$ and %).
  o Is there turnover? Why?
  o Are there unfilled vacancies? Why?
  o What corrective action is proposed?

• Trending of budget and actual expenses over past several years.

• Good management dictates that you operate department within acceptable budget…
  o Being under budget doesn’t mean you are doing a good compliance job!
Budget and Resources

- Who defines what is appropriate?
- Any validation efforts that has been performed to review the potential ROI of your compliance program.
- Specific activities.
  - Sanction screening.
  - Contract management and reporting.*
    - Dealing with Focused Arrangements.
  - Audits (routine and for-cause).

Other Data Points to Trend by Year

- Compliance presentations to senior management & medical staff.
- New and renewed Focus Arrangements.
- Payments made to non-employed physicians without an agreement.
- Payments made to non-employed physicians without evidence of time and effort approval.
- Refunds
- Survey Results
- FWA Referrals and Cases
Elements to Consider in Your Evaluation Efforts

- Hotline Calls
- Education and Policy / Procedures
- Audit/Monitoring
- Potential Areas of Trending Your Coding, Billing Results
- Audit Benchmarking Scorecard
- Annual Audit Work Plan Completion
- Budget Analytics
- Other Data Points to Trend by Year
  - Physician arrangements
  - Survey results

Who should perform a Compliance Program Evaluation?

- Each circumstance probably different
- General Thoughts:
  - Consider an independent external review at some pre-determined interval of time
  - i.e. – every two or three years
  - Contract via the Board and include in budget
  - Report to the Board
  - Assure you have someone doing this who is experienced and bring value – interview them..
  - Utilize findings for improvement and then review again... good auditing approach which can pay dividends in long run..
  - Develop scorecard of good statistics
Privacy and Security Assessments

3 of the 7 Required Elements Are Directly Addressed Through Assessments

Policy and Procedures and Assessments Go Hand in Hand
Audit vs Assessment
Similar But Sometimes Different

• Keeping up and applying all the rules that impact today’s healthcare organizations can be bewildering

• Some rules call for audits but others use the words analysis or assessment

• Many times the differences are a matter of degree and methodology

• HIPAA security requires a risk based methodology but NIST Cybersecurity does not

• OCR performs audits and compliance audits as well as audit monitoring are required

• Audits can mean document production, some assessments are geared towards ‘Yes’ and ‘No’ answers

• Be clear within your own organization as to what differing assessments and audits are used, how and when

Audit vs Assessment
Similar But Sometimes Different

• My slides in this presentation focus on privacy and security ‘assessment’ but I can use my tools to perform three different levels of assessment

  • General
  
  • Advanced
  
  • Audit
HIPAA Security and Privacy Compliance Assessment Requirements

- HIPAA Privacy and Security are two separate, but related sets of regulations, EACH requires assessment.
- They may be assessed in the same or in different projects, but they should be performed together to leverage all concepts across both parts of the organization.
  - e.g. encryption which has both privacy and security considerations.
- For healthcare I recommend a risk assessment methodology, with reporting, followed by a documented, prioritized ‘Risk Management Plan’.
- HIPAA security must be based on a ‘Risk Analysis’ methodology similar to what has been published by NIST and ONC – Privacy is best performed by risk too.
- Other assessment ‘Frameworks’ e.g. NIST Cybersecurity as based on models that are not risk based but basically perform the same functions in a different manner...but are they to be used? Maybe depending upon the size and depth of risk tolerance within your organization.
- ONC/OCR offers a free SRA (Security Risk Analysis) but not one for privacy.
- There is no regulation per se to perform either on a stated interval...but Best Practice, with the least liability, comes from performing both Privacy and Security Risk Analysis annually with continuous monitoring and updating in between.

HIPAA Privacy Compliance Analysis
Regulatory Requirements
Note: None are Direct

164.530 (c)(1) & (i) (1)-(5) (PRA) Administrative Requirements

- (1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
  - It can be deduced that analyzing compliance (be it in a risk based or other analysis) across the entire scope of the privacy rule is a required basic safeguard.
- (1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements.
- The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance.
**Privacy Compliance Gap Assessment**
(in a Risk Analysis Format) Key Components

**A ROBUST Privacy Risk Analysis (PRA) contains questions that explore the following areas**

- Details about the organization’s Privacy Compliance Program
- Privacy (and Breach) policies and procedures and communication
- Patient’s Rights
- Workforce privacy training
- Designated Record Sets
- Incident Management and Breach Notification
- Incident History
- BA Management — Satisfactory Assurances/Questionnaires
- Research

**HIPAA Security Risk Analysis (SRA)**
Regulatory Requirements
Note: These are Directly Mandated

- §164.308(a) Security Risk Analysis (SRA) Administrative Safeguards

- Security Management Process standard, at §164.308(a)(1)(i) in the Administrative Safeguards section of the Security Rule, requires covered entities to “implement policies and procedures to prevent, detect, contain, and correct security violations.”

- Required implementation specification at §164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”

- Required implementation specification at §164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)”

HIPAA Security Risk Analysis (SRA)

- A SRA includes a review of all current policies, procedures, plans and other documentation that support an organization’s HIPAA ‘Information Security Compliance Plan’
  - The assessment ‘framework’ has to be drawn from NIST SP 800 – 66, An Introductory Resource Guide for Implementing the HIPAA Security Rule
  - It is important that IT Asset Inventory be included with documented security controls
  - Increasingly Data Categorization and Flow analysis are required components

- A comprehensive HIPAA Security Gap type Risk Analysis includes an assessment of each HIPAA Security standard, implementation specification, and requirement
  - Document key data and compliance measurements, identify gaps, assess risk, and mutually define a remediation plan based on risk (e.g. Risk management Plan)

- NIST Type Risk Formula: Risk = Threat + Vulnerability + Impact

HIPAA Security Risk Analysis

Key Components

Areas to cover within a SRA include:

- Policies & procedures (P&P) to prevent, detect and correct security violations and define appropriate sanctions
- Assigned security responsibility (i.e. Security Officer and Governance)
- Appropriate and authorized access to PHI and clear termination procedures (and de-provisioning of access)
- Security awareness and training for entire workforce
HIPAA Security Risk Analysis
Key Components

• Security incident procedures
• Contingency and back-up plans
• Periodic evaluation and monitoring of security compliance with continual feedback and remediation
• Ensure compliance of BAs – ‘Satisfactory Assurances’
• Facility access controls
• Workstation use
• Workstation security
• Device and media controls
• Access controls
• Audit controls
• Integrity
• Person or entry authentication
• Transmission security

Assessment Related Content

• Assessments of compliance rarely standalone, certain other supporting documentation is required for full compliance
• Increasingly more controls and documentation of IT Assets and Data cataloguing with flows are needed to comply
• OCR has been heard to say this is a crucial part of security and privacy management
• GDPR and CCPS require them
• What content should accompany compliance assessments?
  • Policies and Procedures (e.g. HIPAA privacy can = 20+ policies, same for security)
  • IT Asset Management – controls, safeguards, other details like versions, etc.
  • Data Cataloguing and Analysis – build upon Legal Health Record and Information Governance foundations
  • Data Flow Mapping – can be visual, e.g. Visio, but does not have to be, can be part of a Data Catalogue
Cybersecurity Has Arisen

• Is there any doubt that an increased mindset about Cybersecurity has arisen throughout the world for electronic information?

• Breach notification now comes from many quarters

• HIPAA has paced most industries in the US with mandated security requirements

• Now general business and industry must follow suit and implement formal security/cybersecurity controls, because of new rules but also civil suit liability

• I differentiate between regulatory security (well defined) and cybersecurity (sort of a hazy definition), although they are descriptive of all the controls and safeguards used to protect the security of electronic information

The Rise of Privacy
Privacy Arises

- Security compliance has always garnered more attention than privacy as it is IT based and obviously important to implement safeguards

- Privacy has not been as well addressed in any sector, except healthcare with HIPAA Privacy which is notable for its strength and scope

- Breach rules tend to be more privacy than security and they have already arisen since we have HIPAA, other Federal rule and State breach laws

- FERPA (student records), SAMHSA 42 CFR Part 2 Substance Abuse and much of the Common Rule for Research are already in place with privacy protections

- Now here comes Privacy with GDPR (General Data Protection Rule – EU, already implemented) and CCPA (California Consumer Protection Act – 2012 implementation) and IoT rules

- Look for the States, especially heavily regulated ones like New York and Massachusetts to follow CCPA. Although there has been some State privacy already and more is certain to come

- GDPR and CCPA can be mapped back to a lot of concepts that HIPAA Privacy Rule already addresses, but these new rules emphasize and cover data not necessarily addressed by HIPAA, even within healthcare entities

- There are exclusions for those that meet HIPAA, but that is dicey to determine

- Could there be a federal privacy law one day? Certainly would be easier to manage than 50 State laws, but who knows…

Choosing Frameworks (Templates) for Privacy and Security Assessments

- Some but not all will be specific to health care industry

- Regardless of which used must identify elements which can be utilized in a evaluation of the compliance program

- Many elements in US will be based upon NIST standards with specific rules such as HIPAA or 42 CFR Part 2

- Choose the appropriate set of assessments for your organization based on reasonableness of approach, size and available resources
Real World Examples of Assessment Templates

• Templates are used to create self contained assessment tools

• There could be an almost endless number of types of templates for compliance activities

• Privacy and security compliance have generated several assessment types

• The next slide lists just some of the templates I and my customers have already created

• Depending upon the assessment tool used building templates can be by the vendor, the customer or a combination of the two

• Useful to have a community of different users submitting templates for use by all users of the assessment tool

Real World Examples of Assessment Frameworks and Topics

Privacy Assessments

• Privacy Risk Analysis General, Advanced & Audit Levels (CE or BA)
• Privacy and Security Walkthrough Assessment
• On-going staff privacy and security Questionnaires
• BAA Component Assessment
• Business Associate (BA) Privacy and Security Compliance Assessment (Satisfactory Assurance)

Security Assessments

• Security Risk Analysis General, Advanced & Audit Level (CE or BA)
• NIST Cybersecurity Framework (primarily, but not exclusively, non-healthcare focused)
• PCI-DSS Assessment – Credit card security
• IT Asset Management Questions
• DFARS NIST 800-171 Assessment

Both Privacy and Security Assessments

• Privacy & Security On-going Program Checklist
Non-HIPAA or Healthcare General Business & Industry Security Assessment

- Non-HIPAA Security includes several competing rule sets. Each with their own assessment template
- Some may require certified auditors, others do not
- This list is only some of the required security standards/rules, there are many others:
  - NIST Cybersecurity Framework – NIST 800-SP-53, ISO and HIPAA Security Rule, among others, basis/crosswalk
  - DFARS NIST SP-171 Non Classified Federal Information
  - PCI-DSS – Credit Cards
  - Sarbanes Oxley – Financial, other general business, accuracy and reporting of financial disclosures and more
  - FINRA – financial (e.g. stock brokers)
  - FERPA – Student Records
  - DoD, Classified Government Information – who knows?
  - Privacy Shield Frameworks data protection requirements when transferring personal data from the EU, Swiss and US in support of transatlantic commerce

GDPR Privacy Assessment

GDPR areas for assessment

- Does GDPR apply? What are use cases that require application of GDPR compliance for an organization?

- Assess what information in an organization is to be considered personal information in what record sets? Use data cataloging to determine:
  - What is ‘Personal Data’ which is expanded to include information related to an identified or identifiable natural person, or “data subject”, which is one who can be identified directly or indirectly, by particular reference to an identifier
  - An identifier includes, but is not limited to: a name, an identification number, location information, online identifier or to one or more data elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person

- Opt-in and consent for personal data use (data use is called ‘processing’)
Non-HIPAA or Healthcare General Business & Industry Privacy Assessment

GDPR areas for assessment

• Determining Data Processors vs Data Controllers (like a CE or a BA)

• DPO (Data Protection Officer) – Required and stricter than a HIPAA Privacy Officer – will this be an outsourced position due to complexity?

• Data Subject Rights – may be assessment or may be specific workflow – CCPAs

• DSAR (Data Subject Access Request) – Similar to HIPAA 3rd party disclosure, TPO and AOD

• Privacy Policy Disclosure – Similar to a HIPAA NPP (Notice of Privacy Practices)

• Breaches – Similar, but of course different to HIPAA breach

• Privacy Impact Analysis (PIA and DPIA)

CCPA
California Consumer Protection Act

• CCPA is similar to GDPR

• I’m still learning it, due to implement January 1, 2020

• Although there is no national right to privacy in the US, this probably will be regulated by the states

• Look for the States, especially heavily regulated ones like New York and Massachusetts to follow CCPA

• Perhaps national legislation one day

• Although there has been some State privacy already and more is certain to come
Best Practice Privacy and Security Assessment Examples

Real World Examples of Assessments and Related Content - Dashboard for Multi-Project Management
Real World Example of a Privacy Assessment

Real World Example of a Walkthrough Assessment
### Real World Example of a Walkthrough Assessment

**Assessment #330 - CHS - 2017 Privacy Visual Assessment - Acute Care Facility**

*Facility:* Another Test CE / *Department:* Inpatient

<table>
<thead>
<tr>
<th>#</th>
<th>Topic</th>
<th>Question</th>
<th>Answer</th>
<th>Comments</th>
<th>Ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incident/Electroshock</td>
<td>Were staff members keeping incidental disclosures of patient information to a minimum in waiting rooms, hallways, and common areas?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NPI - Patient Registration Form</td>
<td>Use the current (2020.12) CHS Notice of Privacy Practices (NHPP) visible and prominently displayed in check-in area; both in Spanish and in English such that patients can take a copy without having to ask for one?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disposing Patient Information</td>
<td>Was patient information ONLY put in locked shredders that were not overflowing; and not in open trash cans, recycle bins or other open containers?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Computer Safeguards</td>
<td>Were appropriate safeguards used for computer screens, workstations on wheels, and medical equipment containing patient information to protect against inappropriate access or use and to limit incidental disclosures?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Real World Example of a NIST Cybersecurity Assessment

**Assessment #322 - NIST Cybersecurity Framework General Business Asses 28 18**

*Facility:* Another Test CE

The tab contains general information about the organization being assessed:

- **Facility:** Another Test CE
- **Department:**
- **Location:**

**Primary Contact:** nobody

**Additional Site Contact:** nobody

**Organization Background:**

---

59

60
Assessment Action Items for Remediation and Risk Calculation

**Assessment Scoring**

Scoring is important, but only for internal use
Assessment Reporting

Reporting by individual case, Analytics for multiple cases

Conclusion

- Key elements of a robust and effective privacy and security compliance program include privacy and security assessment
- Best practices include determining which privacy and security assessments to perform, how often and how to follow-up with an active remediation plan
- In actuality security assessment never ends, but of course projects have to be controlled
- Privacy too, but privacy assessments can be more periodic
- Better to be Proactive than Reactive
THANK YOU ... for your attendance!

Feel Free to Contact
Bret Bissey, MBA, FACHE, CHC, CMPE
Vice President, Chief Compliance Officer at
Gateway Health
bbissey@gatewayhealthplan.com

Kelly McLendon, RHIA, CHPS
CompliancePro Solutions - Managing Director
(321) 268-0320
kmclendon@ComplianceProSolutions.com
www.ComplianceProSolutions.com