

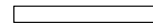


**HCCA Managed Care Compliance
Conference**
January 26, 2020

**Establishing A Best Practice Approach for Your
Compliance, Privacy and Security Programs**

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

Kelly McLendon, RHIA, CHPS
Managing Director, CompliancePro Solutions



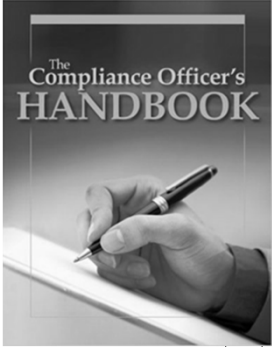
1

Agenda

1. Introduction
2. Compliance Program Best Practices
3. Best Practice Compliance Program Examples
4. Privacy and Security Best Practices
5. Privacy and Security Assessments; Rules, Regs and Best Practices
6. Q&A



2




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

3

3



Kelly McIendon, 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

4

4

Session Goals

- Learn how to utilize, in detail, the elements of the DHHS OIG Model Compliance Program(s) to develop a best practice for your compliance efforts.
- Learn how to utilize the HIPAA Privacy and Security regulations and conduct a program assessment to create a Best Practice standard in your organization.
- Learn how best to formulate Security, Privacy and Compliance education programs in your organization, including a focus on being compliant at the top of the organization, by utilizing market knowledge to stimulate learning.

5

5

Compliance Program Best Practices

6

6

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 – updated April, 2019)

<https://www.justice.gov/criminalfraud/page/file/937501/download>

7

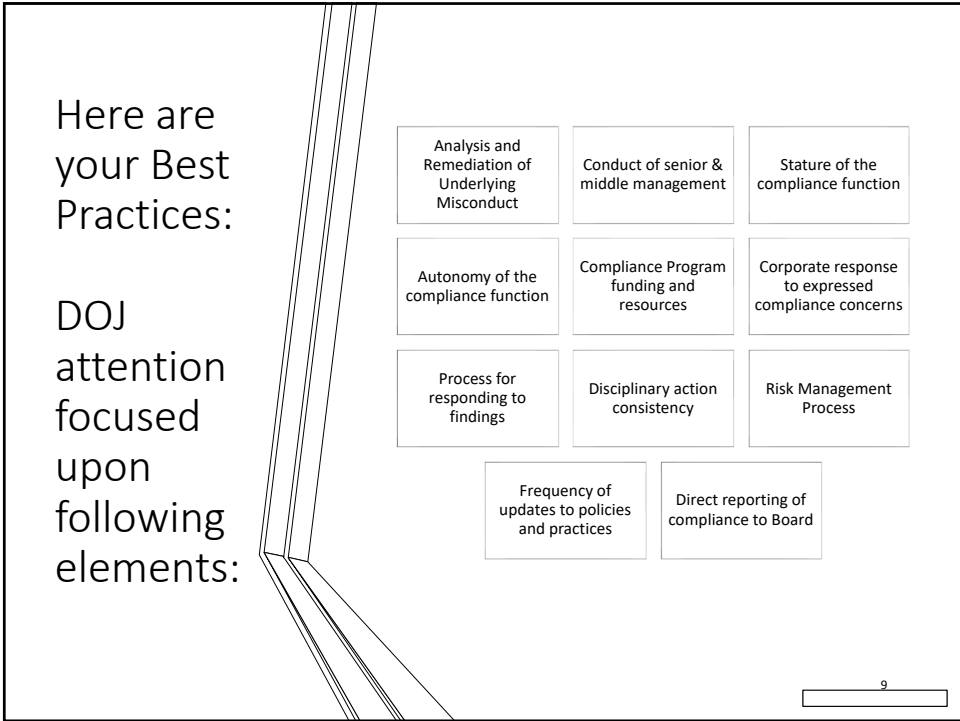
7

DOJ Compliance Program Guidance on Evaluation of Corporate Compliance Programs

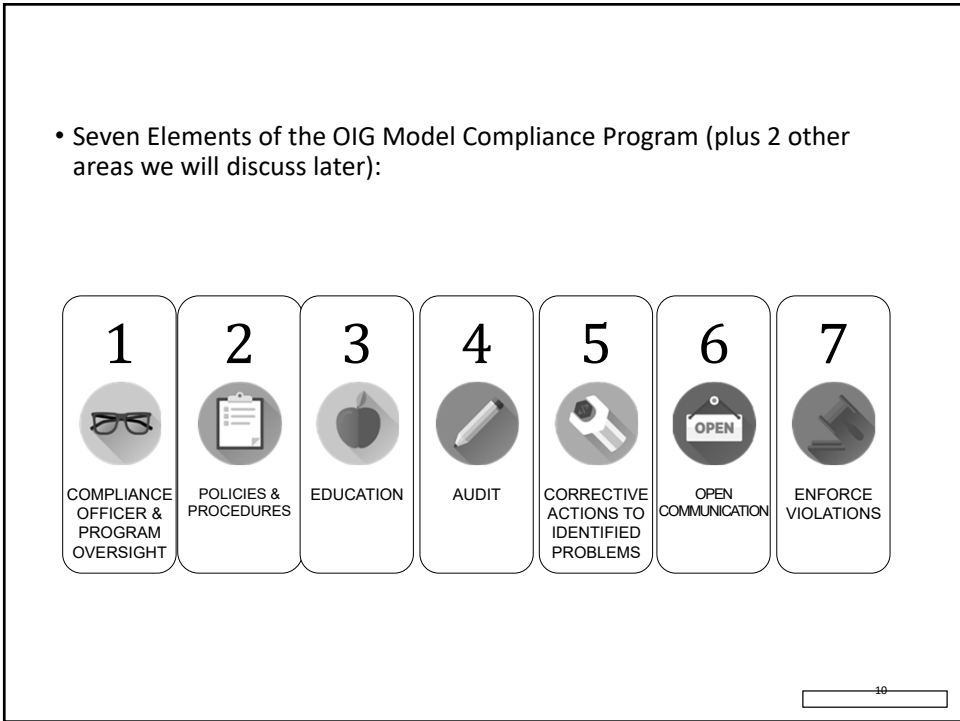
- Not specific to health care industry
- But identifies elements which can be utilized in an evaluation of the compliance program
- Many elements like historical DHHS-OIG Guidance
- The guidance is presented in the form of compliance-focused questions that the DOJ Fraud Division might consider when evaluating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

8

8



9



10

Fraud, Waste and Abuse

- FWA Oversight / Committee
- Special Investigations Unit??
- Systems and Data Analytics?
- Policies?
- Education?
- Reporting Mechanisms?
- Corrective Actions?
- Referral of Cases?
- Investigation Process Timeliness?



11

11

FDR & Delegation Oversight

- Organize an Oversight Committee
- Engage Business Owners
- Required for Medicare Advantage Plans
- Good Idea for all plans
- Utilize the Model Compliance Plan 7 elements
- How are vendors and delegates being monitored?
- What documentation exists for these efforts??

12

12

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

13

13








Compliance Committee Fundamentals

- Chief Compliance Officer chairs
- Minutes of all meeting developed, approved and provided to the Board
- Quorum requirements
- Membership established with Sr Leaders, including CEO
- Compliance Committee Charter
- Expectations of how frequently Committee meets – I like quarterly
- Ground Rules
- A good Compliance Committee requires significant planning

14

14

Best Practice Compliance Elements

-  • Hotline Calls.
-  • Education. —————>
 - Staff.
 - Board.
 - Executives.
-  • Audit Preparation**
-  • Potential Areas of Trending Your Coding, Billing Results.
-  • Annual Audit Work Plan Completion.
-  • Budget Analytics.
-  • Other Data Points to Trend by Year.

15

15

Hotline Calls & Issues – Evaluation



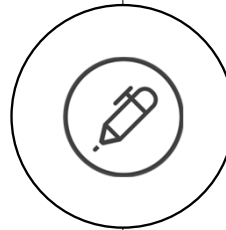
- Do you include just calls or all matters “logged” by Compliance?
- Need to ensure you have a consistent measurement...
- How many of those matters resulted in:
 - Investigations?
 - Remediation?
 - Paybacks?
 - Disciplinary actions?
 - Other?
- Trending data is the key....
- What is your baseline?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

16

16

Education

- How much compliance education is enough?
- Follow DHHS OIG CIA requirement or establish your own expectations?
 - Have Board support.
- Establish standard for different groups – “I like the following:”
 - Staff except housekeeping and food service – 1 hour annually.
 - Executives – 2 hours annually.
 - Physicians – 2 hours annually.
 - Board – 2 hours annually.
 - *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?
 - Answer will tell you about your compliance culture.



17

17

Board Education & Engagement

- Big Compliance Opportunity – take time to develop
- Tailor education 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?

18

18

Chief Compliance Officer

- Ability to 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?
- Executive Session with Audit Committee
- Pre-meeting with Audit Committee Chair prior to Audit Committee meeting

19

19

Chief Compliance Officer

- 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: HCC coding...

20

20

Audit Planning and Preparation

- Audit Season is upon us – none-stop
- Does your organization understand the resources needed?
- Examples to discuss:
 - Program Audits
 - Focused Audits
 - Planned Audits
 - For-Cause Audits
 - 1/3 Financial Audits evolving into Operational Audits
 - Timeliness
 - Quality
 - Etc, etc, etc....
- How do you / can you handle this??

21

21

Corrective Action Plans - Internal

- Create a work-group or committee
- Can you get engagement you need?
- Opportunity to sell the compliance program without people knowing it
- Develop on-going monitoring on identified issues (CAPS)

22

22

Annual Audit Work Plan Completion

- Based upon approved annual work plan.
 - 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.



23

23

Budget Analytics



- Based upon operating and FTE budgets approved by Board or Compliance/Audit Committee.
- Operating budget variance (\$\$ and %).
 - Why a variance? Consultants?
- FTE budget variance (\$\$ and %).
 - Is there turnover? Why?
 - Are there unfilled vacancies? Why?
 - 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...
 - Being under budget doesn't mean you are doing a good compliance job!

24

24

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.
 - Network Adequacy Issues
 - Audits (routine and for-cause).
 - CAPs
 - Delegation Oversight

25

25

Compliance Best Practice Efforts



26

26

Review Your Compliance Program

27

Who should perform a Compliance Program Evaluation?

Although each circumstance is 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

28

28

Compliance Program Best Practices Examples

29

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....

30

30

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?

31

31

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....

32

32

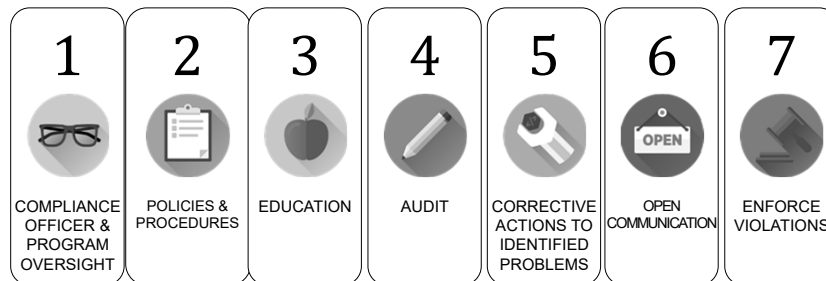
Other Best Practices to Consider

- Figure out what you do well and repeat / Don't over complicate good compliance
- FWA organization and cadence of meetings
- FDR / Delegation oversight committee – well structured
- Test your Hotline
- Tailor your Board and Executive Compliance Education to your organization
- Audits – Preparing Your Organization
- Proactive Corrective Action Plan Efforts (Internal and External CAPS)
- Executive Session with Audit Committee
- Risk Assessment Activities
- Document all efforts – annual compliance report

33

33

3 of the 7 Required Elements Are Directly Addressed Through Assessments



Policy and Procedures and Assessments

Go Hand in Hand

34

34

Privacy and Security Compliance Best Practices

35

35

Privacy Compliance Assessment Including Best Practices

- Key elements of a robust and effective privacy compliance program includes various privacy assessments to measure current practices against both regulatory rules and industry best practices
- In relation to privacy program assessment best practices include:
 - Determining which privacy assessments to perform
 - How often
 - With mechanisms to follow-up with an active remediation plan
 - What are acceptable results
 - What is reporting to whom and when
- With assessments and audits it's much better to be Proactive than Reactive

36

36

Audit vs Assessment Framework and Methodology to Use



- 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
- Set-up Best Practices in your own organization as to what differing assessments and audits are used, how and when

37

37

Privacy Compliance Assessment Types

- Best practices include determining which privacy assessments to perform
- How often to perform
- How to follow-up with an active remediation plan
- Types of assessments include:
 - Full privacy program gap analysis
 - Physical security walkdown
 - Staff Interviews about privacy
 - Business Associate privacy compliance
 - HIM patient access vs 3rd party authorization disclosures
 - Process for performing patient rights, amendment, restrictions, AOD

38

38

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)
- GDPR, CCPA or State Privacy Assessments

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
- State security rule assessments

39

39

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'
- 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

40

40

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

41

41

Key Components of a Privacy Compliance Gap Assessment



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

42

42

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)”
- www.HealthIT.gov/security-risk-assessment

43

43

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

44

44

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

45

45

Best Practices for Privacy and Security Compliance



- Increasingly more controls and documentation of IT Assets and Data Inventorying with Data Flows are needed to comply
- Map/Inventory them yourself or bring in a third party. These processes seem quite manual still
- GDPR, CCPS require them now and coming state privacy (and security) rules will increasingly require
- What content be called out by compliance assessments?
 - Policies, Procedures and Forms (e.g. HIPAA privacy can = 20+ policies, same for security)
 - IT Asset Management – controls, safeguards, other details like versions, etc.
 - Documents like IT Info Security Roadmaps, contingency, back-up, recovery and restoring plans, physical security plans

46

46

Privacy Regulations Expand Best Practice Requirements

- Privacy has not been well addressed in any business sector, except healthcare with HIPAA Privacy which is notable for its strength and scope
- Breach rules are now in all 50 states and privacy rules are just beginning to expand, possibly with explosive growth
- 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, new FERPA student PHI guidance available from OCR
- Now here comes Privacy with GDPR (General Data Protection Rule) – (for EU - EEA), (already implemented) and CCPA (California Consumer Protection Act) – (Jan. 1, 2020 implementation) and CA IoT rules
- GDPR and CCPA can be mapped back to a several concepts that HIPAA Privacy Rule already addresses, but these new rules emphasize and cover data not necessarily addressed by HIPAA, even within healthcare entities
- Will we get a national privacy rule for general business? Maybe, maybe not, it certainly does not seem like a priority

47

47

Privacy Regulations Expand Best Practice Requirements

- So what changes with the increased privacy regulations?
- More detailed cataloging, inventorying and management of information such as gathered by internet cookies, especially if that information is sold or given away
- Detailed policy, procedure, designs, builds and implementation
- Need new or expanded privacy policies and forms, see table of policies
- Also need workflows and hopefully automation for the workflows and data management required for personal information requests from individuals
- And any incidents that may occur that require some kind of investigation and perhaps remediation

48

48

Does CCPA Apply?

- Are one of the three thresholds met?
 - Does this business have annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185?
 - Does the business alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices?
 - Does this business derives 50 percent or more of its annual revenues from selling consumers' personal information?

49

49

CCPA Privacy Best Practices

- **Does CCPA apply?** What are use cases that require application of GDPR compliance for an organization? HIPAA covered information is excluded, but almost always there are other types of information that may not be covered by HIPAA, but will be by CCPA – e.g. information derived from web traffic or cookies
- **Assess what information** in an organization is to be considered CCPA **personal information** in what record sets that has CCPA implications? *Use data inventorying to determine:*
 - What California consumer 'Personal Information' data is included in the data sets your organization manages?
 - What are the organizations DRS (Designated Record Sets) and then other data outside the DRS?
 - Are any other businesses (like BAs, but not necessarily BAs) managing any of this information?
 - Are any other State Laws (for privacy and/or security to be considered)?
 - What format is the information managed in, what storage?

50

50

CCPA Privacy Personal Information

- 1798.140(o)(1) **“Personal information”** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
 - (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
 - (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
 - (C) Characteristics of protected classifications under California or federal law.
 - (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
 - (E) Biometric information.
 - (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.
 - (G) Geolocation data.
 - (H) Audio, electronic, visual, thermal, olfactory, or similar information.
 - (I) Professional or employment-related information.
 - (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
 - (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

51

51

CCPA Privacy Best Practices

- Privacy Policies, Procedures and Forms Created or Updated
- Privacy training updated to include new concepts and processes
- Prepare and implement CCPA Based Privacy Notices
- Opt-out Right for PI sales
- Right of Access, Disclosure and additional details regarding their PI including any 3rd parties it is shared with
- Right of Data Portability
- Right to Deletion and Erasure (The Right to be Forgotten)
- Non-discrimination for invoking Rights
- Breach could establish a private right of action based upon violations of a business’s duty to implement and maintain reasonable security practices and procedures appropriate to risk under CA Law
- Liabilities: Private Right of Action and substantial Civil Fines

52

52

Privacy Best Practices – Policy Update

HIPAA Document #	Master Privacy & Security Templates	GDPR Document #	CCPA Document #	Comments
Privacy				
0s	HIPAA Privacy Rights and Operations Guide			
1s	Privacy Risk Analysis (Gap Assessment) Policy			
2s	Documentation For Security and Privacy Compliance			
6s	Appropriate Access to PHI by Workforce			
7s	Confidentiality of PHI			
8s	Minimum Necessary, Limited DataSet, De-Identification	237g	237c	
9s	Designated Record Set			
10s	Individual (Patient) Access to PHI			
11s	Disclosure of PHI			
12s	Fax Policy			
13s	Request for Amendment of PHI	236g	236c	
14s	Request to Restrict Use and Disclosure of PHI	236g	236c	
15s	Accounting of Disclosures	236g	236c	
16s	Use and Disclosure for Marketing and Fundraising	236g	236c	
17s	Authorization for Use and Disclosure of PHI for Research Purposes			
18s	Audit Controls, Access and Privacy Monitoring	231g	231g	Audits and Evaluation
19sa	Security and Privacy Compliance Master Program (Plan) and Notice of Privacy Practices (Plan)	236g, 238g	236c, 238c	Administrative, physical and technical safeguards

53

53

Privacy Best Practices – Policy Update

20s	Complaints, Privacy Internal and External			
21s	Breach Determination and Reporting Policy		240g	240c
24s	Breach Decision Tree for Omnibus Breach Determination			
25s	Mitigation of Improper Use or Disclosure			
26s	Sanctions, Enforcement and Discipline			
27s	Investigations by HHS - OCR - Other			
29s	BAA Sample Language - CE Perspective			
29sa	BAA Sample Language - BA Perspective			
29sb	BAA Sample Language - BA to Subcontractor Perspective			
30s	NPP - Notice of Privacy Practice Full Template			
30sa	NPP Summary Tri-Fold			
30sb	NPP OCR Model 3 Templates			
	Privacy Notice - Non-Healthcare		229g	229c
33s	Digital Copier and Device Privacy			
34s	HIPAA Privacy & Security Workforce Training		234g	234c
36s	Email and Internet Use Policy			
39s	Business Associate Master Policy		233g	233c
39sa	Business Associate Master Policy for BA or BA Sub-contractor			
40s	Metadata, Non-Text Data, Photo, Video and Audio Management			
47s	Risk Management Plan			
48s	Electronic Signature Policy			
Other document	Privacy Officer Job Description			
126s	Combined Privacy and Security Officer Definition			

See Handouts for Complete Privacy and Security Policy Table

54

54

Privacy Best Practices – Data Inventory Data Elements

- Business Site
- Name of System
- Application Name from Vendor
- Vendor Company Name and Contact Information
- Responsible Department
- List and Description of Data / Documents
- Are System Docs Considered part of Legal Record
- Does System Contain PII
- Data or Document Format(s)
- Retention Timeframe
- Regulator Approval
- Destruction Method

See Handouts for Complete Privacy and Security Policy Table

55

55

Conclusion

- Key elements of a robust and effective privacy and security compliance program include privacy and security assessment of any new or updated rules, including state laws, e.g. CCPA
- Data cataloging and inventory have become mandatory to comply with regulations adequately
- Then update policies, procedures, education and training, as well as be ready to respond to requests or incidents from any new rules

56

56

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

