HITECH WEBINAR

Proposed Modifications to the
HIPAA Privacy, Security and Enforcement Rules

July 20, 2010

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Faculty

- Brian Annulis, JD
  - Partner, Meade & Roach, LLP
  - 773.907.8343
  - bannulis@meaderoach.com
- Ryan Meade, JD
  - Partner, Meade & Roach, LLP
  - 773.472.3975
  - rmeade@meaderoach.com
- Stephen Weiser, JD
  - Of Counsel, Meade & Roach, LLP
  - 312.403.4284
  - sweiser@meaderoach.com

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Objective & Goals of Today's Webinar

The objective of today's webinar is to highlight those provisions of the Proposed Rule that:

- Are surprises
- Go beyond the plain language of HITECH
- May be worthy of comment(s) to HHS

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Objective & Goals of Today's Webinar

- What we are not going to do
  - Today's objective is not to set forth specific recommendations regarding modifications to your existing health information privacy and security program
  - Once the Proposed Rule is finalized, we will host another webinar to provide practical suggestions regarding new policies, procedures, forms and strategies

- We are also not intending to focus specifically on those provisions of the Proposed Rule that address changes required by the plain language of HITECH

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Today's Topics / Agenda

1. Brief Overview/History
2. Delayed Compliance Date(s)
3. Business Associate Transition Provisions
4. Definitional Changes
5. (Sub) Business Associates
6. Business Associate Agreements
7. Deceased Patients
8. *Mens Rea* & Reasonable Cause
9. Marketing
10. No Sale of PHI
11. Research Authorizations
12. Fundraising
13. Notice of Privacy Practices
14. Restrictions on Disclosures to Health Plans
15. Electronic Access
16. Miscellaneous

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

History / Overview

- Health Insurance Portability & Accountability Act of 1996 (HIPAA)
  - Privacy Rule—December 2000, as amended August 2002
    - Effective April 14, 2003
    - Use and disclosure of PHI by covered entities
    - Patient/individual rights
    - Required policies, procedures, forms and BAAs
  - Security Rule—February 2003
    - Effective April 21, 2003
    - ePHI
    - Administrative, physical and technical safeguards
    - Required risk assessment, policies, procedures
  - Enforcement Rule—April, 2003, as amended February 2006
    - Investigative authority
    - CMPs

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

History / Overview

- Health Information Technology for Economic and Clinical health Act (HITECH)
  - Enacted February 17, 2009
  - Direct application of Privacy and Security Rules to BAs
  - Requires new rules, guidances and reports
  - Breach Notification Rule
    - "Unsecured PHI"
  - New CMP structure
  - Effective Dates vary
    - Privacy and Security Rule changes required by February 18, 2010
  - HHS misses deadline
    - Publishes proposed rule regarding modifications to Privacy Rule, Security Rule on July 14, 2010 (Proposed Rule)
    - Allows for 60 day comment period

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

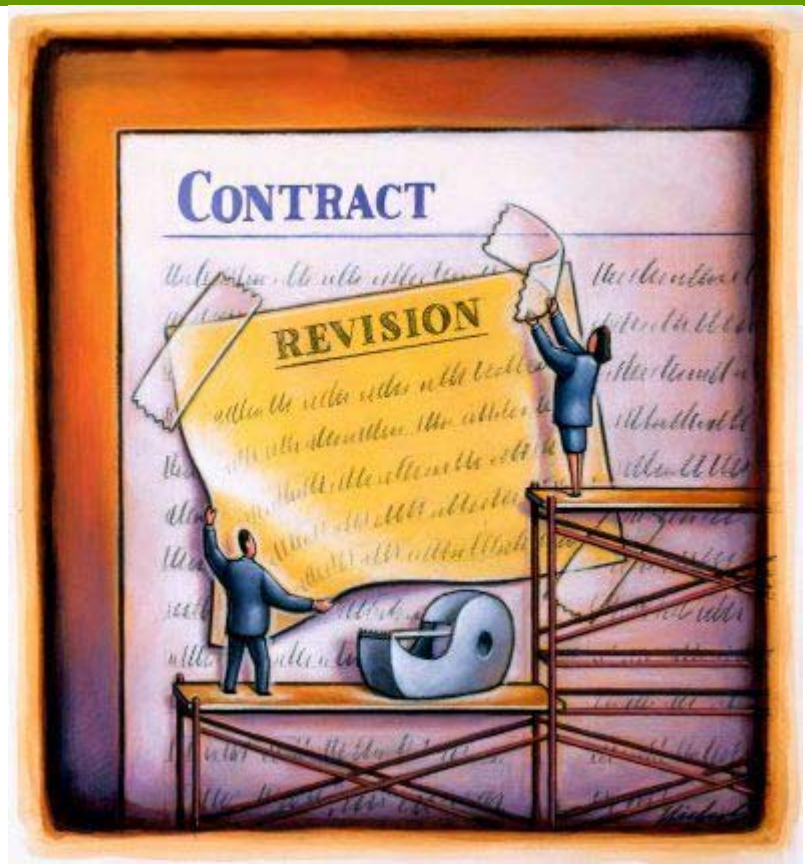
Proposed Rule

- The Proposed Rule codifies many HITECH obligations that are arguably evident from the plain language of the HITECH statutes
  - Application of Privacy Rule and Security Rule to BAs
- Proposed Rule also includes some interpretive surprises
  - Some good
  - Some bad

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Delayed Compliance Date

- HITECH specified a February 18, 2010 effective date for many of the changes/expansions
- Many CEs and BAs began in earnest to attempt to address those obligations prior to February 18, 2010
  - Amended existing BAAs, and/or
  - Incorporated HITECH obligations into new BAAs
- Others waited in earnest for guidance from HHS
  - And waited, and waited, and waited….
- February 18, 2010 came and went



AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Delayed Compliance Date

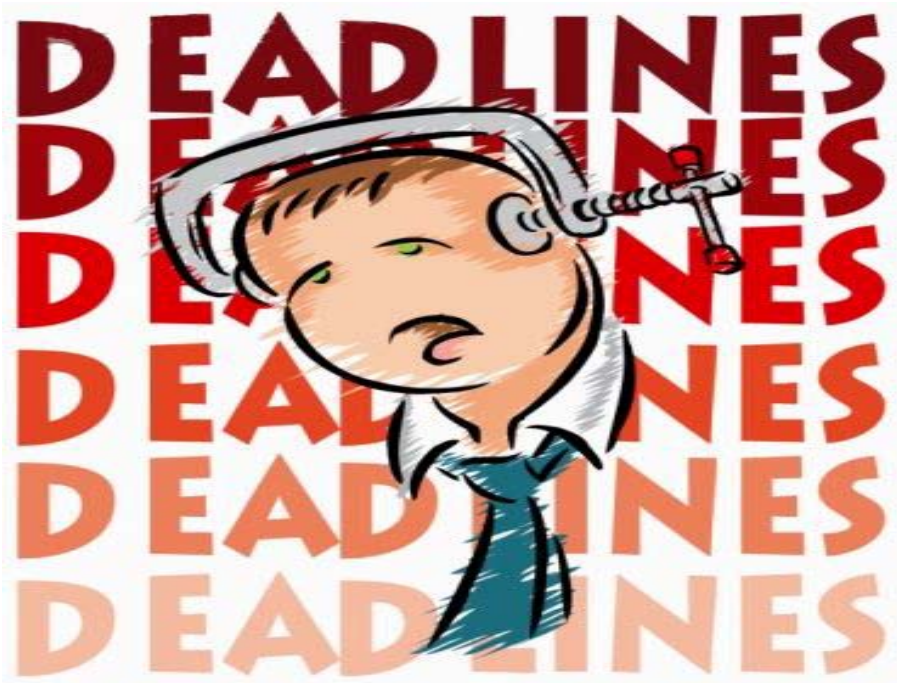
- In the Proposed Rule, HHS acknowledges its tardiness

- Proposes not to enforce final rule until 180 days after the final rule is effective
  - Would not expect final rule to be published until late 2010/early 2011, with an effective date 60 days thereafter.
  - Thus, Compliance Date = 240 days after publication of the final rule
  - As a practical matter, this affords CEs and BAs another year (plus) to implement the changes set forth in the Proposed Rule
  - Delayed Compliance Date will apply to most HITECH Privacy Rule and Security Rule changes (but not Enforcement Rule standards)

- Welcome news, but don't delay too long to develop your compliance strategy

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Business Associate Transition Provisions



AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Business Associate Transition Provisions

BAA "transition provision" provides significant relief for CEs and BAs

Proposed Rule provides:

- Only BAAs that are (1) compliant with the existing rule prior to the Effective Date of the final rule (60 days after publication) are eligible for transition period, and (2) only if the BAA is not modified or renewed from the Effective Date (60 days after publication) and until after the Compliance Date (240 days after publication).

- BAAs that are compliant with existing rule are deemed compliant until the earlier of (1) the date renewed or modified after the Compliance Date (240 days after publication) or (2) one year after the Compliance Date.

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Changes to Definitions

"Business Associates" would include:

1. Patient Safety Organizations,
2. Health Information Organizations, E-prescribing gateways, and RHIO's and
3. Subcontractors.

- Electronic Media – includes digitally stored PHI including digitally stored voice mail.

- Marketing – discussed in later part of this presentation.

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

(Sub) Business Associates

- As noted, plain language of HITECH requires direct application of certain Privacy Rule and Security Rule provisions to BAs
  - BA health information privacy and security obligations no longer just a function of BAA

- But, in Proposed Rule, HHS goes beyond plain language of HITECH to propose that a BA will also include a sub-contractor
  - "The proposed provisions avoid having privacy and security protections for [PHI] lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity." 75 Fed Reg 40868, 40873 (July 14, 2010)

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

(Sub) Business Associates

HHS asserts broad authority in applying BA requirements to subcontractors that many believe are beyond its statutory authority:

- HHS interprets HITECH and the Privacy Rule permitting rules that would required “downstream entities” that work at the direction of or on behalf of a BA and handle PHI to comply with the Privacy Rule. See 75 Fed Reg at 40873 for full text.
- At time of initial promulgation of Privacy Rule, there was significant debate as to whether HHS had the authority to require CEs to enter into Bas
- Proposed Rule goes one step further

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

(Sub) Business Associates

HHS asserts broad authority in applying BA requirements to subcontractors that many believe are beyond its statutory authority:

- It took Congress almost 15 years to extend the Privacy Rule to BAs but HITECH does not specifically extend to subcontractors;
- Does HHS have statutory authority to extend Privacy Rule to BA subcontractors?
- HHS' position is that it has "broad authority" to interpret HIPAA and HITECH.

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

(Sub) Business Associates

Practical ramification of this proposed change are far-reaching

- BAs will not only need to adopt health information privacy and security programs, conduct a required risk assessment, and amend existing BAAs with current CEs, they will also need to identify and enter into sub-BAAs with their subcontractors

- For all practical purposes, BAs will effectively be subject to the same requirements of CEs with respect to their subcontractors. See 75 Fed. Reg. 40889

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

(Sub) Business Associates

<u>Practical ramification of this proposed change are far-reaching</u>

- Implications:
  - Will/should BAs appoint/hire Privacy Officers and Security Officers?
  - How will BAs approach renegotiation of BAAs with CEs?
    - CEs don't want multiple forms of BAAs in place with their BAs
    - But, BAs with multiple subs also will not want multiple forms of BAAs in place with their CEs
    - Indemnification?

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

(Sub) Business Associates

HHS requests comments on this proposed change

- Business Associates with multiple subcontractors (or a subcontractor for BAs), may want to accept that invitation.
- Comments that point out practical difficulties of compliance and companies that will avoid servicing the health care industry may have the strongest points.

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Business Associates and Business Associate Agreements

Proposed Rule would impact BAAs, as follows:

1. No obligation for CEs to report to HHS when termination of a BAA is not feasible
2. BAs now have direct liability for CMPs and CEs and BAs have duties to report breaches involving unsecured PHI to HHS
3. BA not in compliance with Privacy Rule if BA knows of violation by sub-BA and fails to cure or terminate sub-BAA

BAAs will need to address this new environment

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Business Associates and Business Associate Agreements

HHS proposes certain modifications to BAAs "to align the requirements for the business associate contract with the requirements in the HITECH Act and elsewhere" within the Privacy Rule and Security Rule, including:

- comply with the Security Rule with regard to ePHI
- report breaches of unsecured protected health information to CEs,
- comply with applicable requirements of the Privacy Rule that apply to the CE in the performance of such obligation.
- required to enter into BAAs, or other arrangements with their BA subcontractors in the same manner that CEs are required to enter into contracts or other arrangements with their BAs.

Note: BAs will no longer require provision that BAs obtain satisfactory assurances from their subcontractor

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Deceased Patients

- HHS proposes to modify the Privacy Rule to specify that Privacy Rule protections expire 50 years after your death

- Also, expands Privacy Rule to permit PHI disclosures to persons involved in decedents care under 45 CFR 164.510(b)

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Mens Rea & Reasonable Cause

HITECH and HITECH Enforcement Rule establish 4 categories/tiers of health information privacy and security violations for purposes of imposing CMPs

1. Did not know and by exercising reasonable diligence would not have known of a violation
2. Violations due to reasonable cause, but not willful neglect
3. Violations due to willful neglect, but timely corrected
4. Violations due to willful neglect, but not timely corrected

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Mens Rea & Reasonable Cause

Proposed Rule sets forth some interesting/beneficial examples regarding imputed knowledge of CE and BA employees

- "A hospital employee accessed the medical record of his ex-spouse while he was on duty to discover her current address for a personal reason, knowing that such access is not permitted by the Privacy Rule and contrary to the policies and procedures of the hospital. HHS's investigation reveals that the [CE] had appropriate and reasonable safeguards regarding employee access to medical records, and that it had delivered appropriate training to the employee." 75 Fed Reg 40879

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Mens Rea & Reasonable Cause

- HHS concludes:
  - The "did not know" category is implicated with respect to the CE ☺
  - *Mens rea* element of knowledge cannot be established
  - EE's act is attributed to CE, but EE's knowledge cannot be imputed to the CE because EE was acting adversely to CE
    - Any time an EE acts contrary to CE's health information privacy and security program, would not employee be acting adversely to CE?
- But, may not alleviate CE's reporting obligation under Breach Notification Rule

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Mens Rea & Reasonable Cause

- Conversely, HHS proposes to remove a current line of reasoning in which CE avoids liability for the acts of its BA agent, if there is a valid BAA and the CE did not know of the violation by the BA.

> "We propose to remove this exception to principal liability for the [CE] so that the [CE] remains liable for the acts of its [BA] agents, regardless of whether the [CE] has a compliant BAA in place. This change is necessary to ensure, where the [CE] has contracted out a particular obligation under the HIPAA Rules, . . ., that the [CE] remains liable for the failure of its [BA] to perform that obligation on the [CE]'s behalf." 75 Fed Reg 40879

- "[CE]'s are customarily liable for the acts of their agents under agency common law." [?] 75 Fed Reg 40880

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

How to Reconcile?

- If CEs/BAs do the right things (e.g., P&Ps, training), then they are NOT responsible for the wrongful acts of their employees/workforce?

BUT

- Always responsible for wrongful acts of BA?
  - What about direct liability/responsibility by BA?
  - Emphasize need for continued indemnification by BA in BAA?

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Marketing

- HITECH limits health-related communications that may be made by CE about third party products without authorization (i.e., communications excepted from the definition of "marketing")
- If covered HCP receives remuneration in exchange for health-related **treatment** communications, no authorization required but must:
  - Adhere to notice and opt-out requirements
  - HCPs must amend its NPP to include a statement that HCP intends to send subsidized treatment communications, as well as an opportunity for individual to opt-out of receiving such communications
  - Opt out option must be "simple, quick and inexpensive"

- If covered CEs receive remuneration in exchange for health-related **HCO** communications, authorizations are required.

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Marketing

HITECH includes exception for communication about alternative drug or biologic that is currently being prescribed so long as the remuneration is reasonable

- HHS requests comments on whether this should include communications about generic alternatives
- Also, should reasonable remuneration be limited to actual cost? Reasonably related costs?

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

No Sale of PHI

- Broadly speaking, HITECH bans sale of PHI without individual authorization, with some exceptions
  - Exceptions: public health; research; treatment; sale, transfer or merger of CE; services rendered by BA; individual access; other purposes determined by HHS
- If authorization required, authorization form must include a statement to the effect that CE is receiving remuneration in exchange for PHI
- No re-disclosure by recipient unless authorization provides as much

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

No Sale of PHI

- Exceptions
  - Disclosures of PHI involving Remuneration for Public Health Purposes
    - Also, PHI disclosed via a LDS for research does not require an authorization. Logical, as Privacy Rule currently permits use and disclosure of a LDS of PHI for public health purposes without authorization
  - Disclosures of PHI involving Remuneration for Research Purposes
    - PHI disclosed for research purposes does not require an authorization
    - But, remuneration to be received by the CE for disclosure of PHI for research must be limited to "**a reasonable, cost-based fee to cover the cost to prepare and the PHI for research purposes**."
    - PHI disclosed via a LDS for research also does not require an authorization. Logical, as Privacy Rule currently permits use and disclosure of a LDS of PHI for research without authorization

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

No Sale of PHI

- Exceptions
  - Disclosure of PHI involving Remuneration for Treatment and Payment Purposes
  - Disclosures of PHI involving Remuneration for HCO Purposes
    - Sale, merger or consolidation of PHI
    - Note: No explicit proposed exception to allow for disclosure of LDS of PHI for HCO purposes

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Implications of No Sale of PHI

Implications?

- May have significant practical consequences for some health care providers
- Procurements contracts with device manufacturers and pharmacy often involve rebates and discounts in exchange for disclosure of LDS of PHI.
- Currently permitted under the Privacy Rule, but no proposed exception under Proposed Rule

Consequences?

- Catch all exception?—allows for disclosures involving remuneration without authorization for any other purpose permitted by the Privacy Rule, but only if the remuneration is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI. In most cases, the allocated discount/rebate exceeds the cost of preparation and transmission
- Disclosure of de-identified health information? What impact will that have on value of discount/rebate?

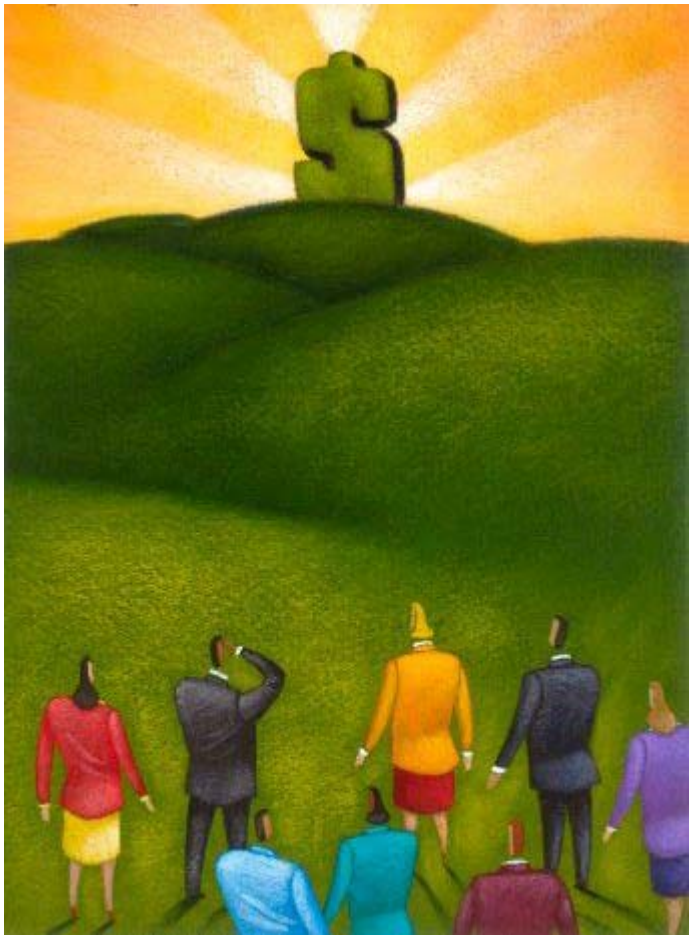
AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Research Authorizations

- Proposed Rule would allow compound authorizations for research (conditioned) AND tissue/blood banking (unconditioned)
  - But, authorization must clearly differentiate between conditioned and unconditioned research activities

- HHS is considering modifying its prior position on study-specific authorizations

Fundraising



- Fundraising communications must include a clear and conspicuous opt-out opportunity
- Opt-out opportunity must not be unduly burdensome
- No fundraising communications to persons who have opted-out (versus reasonable efforts)
- Amend NPP to specify opt-out right
- Solicits public comment on targeted fundraising

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Notice of Privacy Practices

- Propose to amend NPP to:
  - Include a statement that describes the uses and disclosures of PHI that require an authorization and to provide that other uses and disclosures not described in the notice will be made only with individual authorization
  - Specify if CE will receive any subsidization for treatment communications
  - Specify if CE will engage in fundraising with opt-out opportunity
  - Accommodate restriction requests to health plans for treatment to be paid for out-of-pocket

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Notice of Privacy Practices

HHS requests public comment on

- NPP modifications in regard to breach notification
- Health plan NPP distribution obligations

Restrictions on Disclosures to Health Plans

- Individual has right to determine what items/services to be covered by the restriction request

- Request for comment on how to implement
  - Obligation, if any, to inform downstream providers about restriction request
  - Does individual's subsequent request to submit payment to Health Plan revoke prior restriction request?
  - Whether direct payments are included in "out of pocket" costs?
  - How to implement in regard to HMOs (patient may not have option to pay out of pocket)? Must patient go out of network?

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Electronic Access

- Proposes to require electronic copy of all PHI maintained electronically, even if not part of an EHR

- HHS requests public comment on
  - determining reasonable fees for providing electronic access
  - Time period to provide electronic access

Miscellaneous

Expand 164.512(b) to permit disclosure of school immunization with authorization to schools in states with school entry laws

Take-away Points

- HHS is encouraging the public to comment on the Proposed Rule – consider giving your opinion.

- While no one knows how the Proposed Rule will be finalized, it is highly likely that within one year, CEs will need to:
  - Undertake a new BAA initiative
  - Redraft Notice of Privacy Practices

- BAs need to develop privacy and security compliance programs and begin the organization of a sub-BA contracting initiative

AEGIS
COMPLIANCE & ETHICS CENTER, LLP

Follow-Up

- Questions?

questions@aegis-compliance.com

audiocourses@aegis-compliance.com

- Next Lecture:

Once final rules are published,
we will host another webinar

AEGIS
COMPLIANCE & ETHICS CENTER, LLP