2014 Legal Updates

2014 PCC Users Conference

July 18, 2014

Alexa H. Clauss, Esq.
Anne E. Cramer, Esq.
Shireen T. Hart, Esq.

Primmer Piper Eggleston & Cramer PC

www.primmer.com

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Outline

I. HIPAA Breach Reporting and Enforcement Update

II. Baseline Privacy/Security Recommendations

III. HIPAA and Student Immunizations

IV. HIPAA and FERPA

V. Employment Law Update

VI. Further Discussion Topics as Time Allows

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

I. HIPAA Breach Reporting and Enforcement Update

- Revisit what a breach is
- Discuss when to provide notice of breach to patient
- Review most recent aggregated enforcement data
- Review recent cases
- Review lessons learned

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Breach Definition – Practical Review

- Unsecured (unencrypted) PHI
- Acquisition, access, use or disclosure of PHI in manner not permitted under Privacy or Security Rules

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Breach Definition – Practical Review

- Excludes:
  - Unintentional access by workforce member
  - Inadvertent disclosure by authorized person within same entity
  - Disclosure where unauthorized person would not reasonably retain it

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

HIPAA Breach Standard

An impermissible use or disclosure of PHI is **presumed to be a breach** unless covered entity or business associate, demonstrates that there is a **low probability that the PHI has been compromised**.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

4 Factor Risk Assessment

- Nature and extent of PHI involved, including the types of identifiers and likelihood of re-identification
- The unauthorized person who accessed or used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Notification Procedures

- **When**
  - Within 60 days of discovery
  - Outer limit

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Notification Procedures

- **To whom**
  - Individual or personal representatives

Notification Procedures

- **Content**
  - Notification must:
    - be written in plain language
    - describe what happened and date of discovery
    - describe types of PHI involved
    - outline any steps that should be taken by individual to protect themselves
    - describe what Covered Entity is doing to mitigate harm and protect against future breach
    - outline contact procedures

Notification Procedures

- **How**
  - Generally first class mail, or by email, if prior agreement, to individual or personal representative
    - If contact information is insufficient for 10 or more individuals, could provide substitute notice (newspaper or conspicuous posting on provider's website)
  - If urgent situation, notice by telephone or other means

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Notification Procedures

- **If more than 500**
  - If 500 or more residents of one state affected by a breach, notification by prominent media outlet and to Secretary of U.S. Department of Health and Human Services (HHS)
  - If there are 500 or more affected individuals by a breach, but not 500 from one state, Secretary of HHS must be notified concurrently with individual notifications

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Notification Procedures

- **If fewer than 500**
  - Providers need to maintain an annual log of breaches involving fewer than 500 people and provide it to the Secretary as specified on the HHS website within 60 days after the end of each calendar year (by March 1) of year breaches were discovered

Breach Mitigation / Prevention

- Offer credit monitoring to affected individuals
- Designate person/persons to handle inquiries
- Review/revise HIPAA privacy and security procedures, including incident response plan
- Train workforce on safeguarding PHI
- Encrypt portable media with PHI
- Require employees to change passwords
- Increase physical security
- Sanction workforce member responsible for breach

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Enforcement

- The Office of Civil Rights ("OCR") must investigate all cases of possible willful neglect and conduct

- OCR conducts a preliminary review of every complaint received and proceeds with an investigation where possible HIPAA Rule violation

- Be aware of the potential for criminal indictment if intentional violations

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

HIPAA Breach Reports

Please note difference between notice of breach to affected individuals and report of breach to OCR.

- US Department of Health and Human Services Office for Civil Rights ("OCR")

- Breaches are divided into 2 categories, **large breach** and **small breach**.

  Large = breach affecting 500 or more individuals

  Small = breach affecting fewer than 500 individuals

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Data for 2012*

- OCR received 21,194 reports of small breaches that occurred between 1/1/12 and 12/31/12
- Affected ~165,135 individuals
- 3,576 reported by health plans
- 17,562 reported by health care providers

*Reporting deadline for small beaches in 2013 was March 2014.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Most common causes of breach incidents affecting fewer than 500 individuals (2012 data)

- **Unauthorized access or disclosure** (15,695 reports affecting 58,882 individuals)
- **Unknown/other** (2,945 reports affecting 19,483 individuals)
- **Theft** (1,063 reports affecting 50,272 individuals)
- **Loss** (774 reports affecting 19,518 individuals)
- **Hacking/IT incident** (514 reports affecting 10,534 individuals)
- **Improper disposal** (203 reports affecting 6,446 individuals)

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Location of data that was breached (2012 data)

- 12,946 involved paper records
- 1,694 reports involved an electronic medical record
- 711 reports involved desktop computer
- 220 reports involved laptops
- 4,398 did not identify location of data that was breached

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Most common unauthorized disclosure: misdirected communications (2012 data)

- Clinical or claims record was mistakenly mailed or faxed to another individual
- Test results sent to wrong patient
- Files attached to wrong patient record
- Emails sent to wrong individuals

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Responses by covered entities (2012 data)

- Fixing software glitches
- Revising policies and procedures
- Training or retraining employees who handle protected health information

OCR investigations of Self-Reported Breaches

- 100% of breaches affecting more than 500 individuals are investigated by OCR.
- OCR opens investigations into numerous breaches affecting fewer than 500 individuals.

Please be mindful of difference between reports by covered entities to OCR versus complaints by patients, etc. to OCR.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

OCR Investigation closures

- Voluntary compliance by the covered entity
- Corrective action and technical assistance
- Resolution agreements
- Finding of no violation

Third-Party HIPAA Complaints to OCR
(e.g., complaints by patients)

YEAR	COMPLAINTS RECEIVED
2003	3,742
2004	6,534
2005	6,866
2006	7,362
2007	8,221
2008	8,729
2009	7,587
2010	8,764
2011	9,022
2012	10,454
2013	12,915

Types of Affected Covered Entities

Most common types of covered entities required to take corrective action to achieve voluntary compliance (in order of frequency):

- Private Practices
- General Hospitals
- Outpatient Facilities
- Health Plans
- Pharmacies

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Hospital Implements New Minimum Necessary Polices for Telephone Messages

- Covered Entity: **General Hospital**
- Issues: **Minimum Necessary; Confidential Communications**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Pharmacy Chain Enters into Business Associate Agreement with Law Firm

- Covered Entity: **Pharmacy Chain**

- Issue: **Impermissible Uses and Disclosures;**

  Business Associates

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Private Practice Implements Safeguards for Waiting Rooms

- Covered Entity: **Private Practice**
- Issue: **Safeguards; Impermissible Uses and Disclosures**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Private Practice Revises Access Procedure to Provide Access Despite an Outstanding Balance

- Covered Entity: **Private Practice**
- Issue: **Access**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Private Practice Ceases Conditioning of Compliance with the Privacy Rule

- Covered Entity: **Private Practice**
- Issue: **Conditioning Compliance with the Privacy Rule**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Private Practice Revises Process to Provide Access to Records

- Covered Entity: **Private Practices**
- Issue: **Access**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Physician Revises Faxing Procedures to Safeguard PHI

- Covered Entity: **Health Care Provider**
- Issue: **Safeguards**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Case Example: Dentist Revises Process to Safeguard Medical Alert PHI

- Covered Entity: **Health Care Provider**
- Issue: **Safeguards; Minimum Necessary**

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Lessons Learned – 1) Risk Analysis and Risk Management

- Ensure thorough security risk analysis and risk management plan

- Identify and address potential risks and vulnerabilities to all ePHI regardless of location or media

- (computer hard drives, digital copiers, equipment with hard drives, USB drives, laptops, mobile phones, transmitted across networks.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Security Risk Assessment (SRA) tool

- HIPAA requires covered entities to conduct risk assessment of their healthcare organization.

- Tool announced in March 2014 helps health care providers in **small to medium sized offices** conduct risk assessments of their organizations.

- The application, available for downloading at ***www.HealthIT.gov/security-risk-assessment*** also produces a report that can be provided to auditors.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Lessons Learned - 2) Security Evaluation

- Conduct **security evaluation** when there are operational changes

- Conduct **technical evaluation** when there are technical upgrades

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Lessons Learned – 3) Security and Control of Portable Electronic Devices

- Ensure that PHI stored and transported on portable devices is properly safeguarded, including through encryption.

- Policies and procedures governing receipt and removal of portable devices and media containing PHI and how to secure when off-site.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Lessons Learned – 4) Proper Disposal

- Implement clear policies and procedure for proper disposal of PHI in all forms.

Recent Vermont case.

Lessons Learned – 5) Physical Access Controls

- Ensure physical safeguards are in place to limit access to facilities and workstations that maintain PHI.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Lessons Learned – 6) Training

- Ensure training on organization's privacy and security policies and procedures, including appropriate uses and disclosures of PHI.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

II. Baseline HIPAA Compliance Documents / Policies

- Privacy
- Security
- Business Associates
- Breach
- Insurance Coverage Review

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Baseline HIPAA Compliance Documents/Policies

Privacy

- Notice of Privacy Practices (updated!) and policy/procedure for patient acknowledgement
- Confidentiality Policy addressing appropriate circumstances for use and disclosure of PHI
- Minimum Necessary Policy for non-treatment related use or disclosure of PHI

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Baseline HIPAA Compliance Documents/Policies

Privacy

- Patient rights to access, amend, obtain accounting, file complaints, etc.
- Employee training materials and policy on frequency of training
- Employee Discipline Policy

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Baseline HIPAA Compliance Documents/Policies

Security

- Detailed Security Risk Assessment
- Documentation of encryption (justification if no encryption)
- Security Management Policy, including provisions for audit logs, access reports and security incident tracking reports
- Facility Security Plan (addresses administrative, physical and technical safeguards)
- Encryption and Decryption Policy
- System User Access Policy

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Baseline HIPAA Compliance Documents/Policies

Business Associates

- Identify Business Associates and execute Business Associate Agreements (BAAs) with all
- Deadline for updating BAAs = September 23, 2014!
- Consider level of risk exposure/request:
  - Privacy and Security Policies
  - Security risk analysis
  - Subcontractor agreements

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Baseline HIPAA Compliance Documents/Policies

Breach

- Security Incident and Breach Review Policy, including risk assessment and reporting procedures

Insurance Coverage Review

- Privacy/Security breach related claims rivaling payouts for professional liability

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

III. HIPAA and Student Immunizations

- Most states have "school entry" laws: prohibiting a child from attending school unless the school has proof that the child has been appropriately immunized.
- HITECH Act revised HIPAA's Privacy Rule to make it easier for parents/guardians to get the necessary information about their child's immunizations provided to their child's school.
- If the parent agrees orally or in writing, a covered entity may disclose immunization data to a school.
- A HIPAA-compliant authorization is no longer needed.
- Ensures schools are able to receive the necessary documentation of immunization in a timely manner and admit children without undue delay.

Required Documentation

- Must only make clear that agreement was obtained.
- Examples
  - If parent/guardian submits a written or email request to pediatrician to disclose proof that his/her child has been immunized to the child's school, a copy of the request would suffice as documentation of the agreement.
  - If parent/guardian calls the pediatrician and requests over the phone that proof of his/her child's immunization be disclosed to the child's school, a notation in child's medical record of the phone call would suffice.
  - Documentation need not include signature of parent/guardian or any other elements required for written HIPAA authorization.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

State law

- If state law **requires** a covered health care provider to disclose proof of a student's immunizations directly to a school without the affirmative permission of a parent or guardian, the Privacy Rule permits a disclosure limited to the relevant requirements of that law.

- Where a school is not subject to a school entry law but seeks proof of immunization of students, a covered health care provider may either provide the proof of immunization to the parent/guardian to give to the school, or obtain the parent's/guardian's written authorization to provide the requested information directly to the school.

IV. FERPA AND HIPAA

- Relationship between the *Family Educational Rights and Privacy Act* (*FERPA*) and the *Health Insurance Portability and Accountability Act of 1996* (*HIPAA*) Privacy Rule.

- How these two laws apply to records maintained on students.

- Certain disclosures that are allowed without consent or authorization under both laws, especially those related to health and safety emergency situations.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Overview of *FERPA*

- *FERPA* is a Federal law that protects the privacy of students' "education records."
- *FERPA* applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education.
- This includes virtually all public schools and school districts and most private and public postsecondary institutions, including medical and other professional schools.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Where *FERPA* and *HIPAA* May Intersect

- When a school provides health care to students in the normal course of business, such as through its health clinic, it is also a "health care provider" as defined by *HIPAA*. If a school also conducts any covered transactions electronically in connection with that health care, it is then a covered entity under *HIPAA*.

- However, many schools, even those that are HIPAA covered entities, are not required to comply with the HIPAA Privacy Rule because the only health records maintained by the school are "education records" or "treatment records" of eligible students under FERPA, both of which are excluded from coverage under the HIPAA Privacy Rule.

Generally, the *HIPAA* Privacy Rule does not apply to an elementary or secondary school.

- It is not a *HIPAA* covered entity; or
- is a *HIPAA* covered entity but maintains health information only on students in records that are by definition "education records" under *FERPA* and, therefore, is not subject to the *HIPAA* Privacy Rule.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Application of *FERPA* to health records for students maintained by elementary or secondary schools

Students' immunization and other health records are "education records" subject to *FERPA*.

Parents have a right under *FERPA* to inspect and review these health and medical records.

Records may not be shared with third parties without written parental consent unless the disclosure meets an exception to *FERPA*'s general consent requirement.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Circumstances in which the *HIPAA* Privacy Rule might apply to an elementary or secondary school

- Where the school is a *HIPAA* covered entity and is not subject to *FERPA*.
- Most private schools at elementary/ secondary school levels do not receive funding from US Department of Education
  -- not subject to *FERPA*.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Elementary or secondary school student health records maintained by a health care provider that is not employed by a school

When outside parties provide services directly to students and are not employed by, under contract to, or otherwise acting on behalf of the school – records are not "education records."

Under certain circumstances *FERPA* permits an eligible student's treatment records to be disclosed to a third-party health care

An eligible student's treatment records may be shared with health care professionals who are providing treatment to the student, including those who are not part of the educational institution, if disclosed only for the purpose of providing treatment to the student.

An eligible student's treatment records may be disclosed to a third-party health care provider when the student has requested that his or her records be "reviewed by a physician or other appropriate professional of the student's choice."

Where *HIPAA's* Privacy Rule applies, it allows a health care provider to disclose PHI about a student to a school nurse or physician

The Privacy Rule allows providers to disclose PHI about students to school health care providers for treatment purposes, without the authorization of the student or student's parent.

Where the *HIPAA* Privacy Rule applies, in most cases it allows a health care provider to disclose PHI about a troubled teen to the parents of the teen

- *HIPAA* Privacy Rule generally allows a covered entity to disclose PHI about the child to the child's parent, as the minor child's personal representative, when the disclosure is not inconsistent with state or other law.

- In some cases, such as when a minor may receive treatment without a parent's consent under applicable law, the parents are not treated as the minor's personal representative.

Disclosures to law enforcement, family members, or others if the provider believes the patient presents a serious danger to self or others

Privacy Rule permits the disclosure of PHI, when the provider has a good faith belief that the disclosure:

(1)is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others and

(2)is to a person(s) reasonably able to prevent or lessen the threat.

This may include, depending on the circumstances, disclosure to law enforcement, family members, the target of the threat, or others who the provider has a good faith belief can mitigate the threat.

The disclosure also must be consistent with applicable law and standards of ethical conduct.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

V. Employment Law Update

- Recent Wage and Hour Developments
- National Labor Relations Board Update
- "Bring Your Own Device" Considerations

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Fact Pattern

ABC Practice is planning to expand, and unbeknownst to her manager, a receptionist, Jane, has been working on a related project from her home computer. Jane has been logging onto the Practice's network, and she has also been saving her work on her home computer. Jane did not log out of the Practice's network, and when her son used the computer the next day, her son accidentally downloaded a virus into the Practice's network. When using the home computer, Jane's babysitter reviewed the Practice's non-public plans to expand.

Jane entered time spent working from 8-11 p.m. on Monday and Tuesday on her timeslip, putting her total hours for the week over 40. The Practice tells her it will not pay her because she was working after hours without permission, and besides, she receives a set salary and does not get paid overtime.

Later that week, she posts to her Facebook status, "ABC Practice refuses to pay me for the long hours I've been putting in on this project. It's bu!!s*t!!!" Two co-workers "like" her post. The Practice Manager, who is friends with the Receptionist, shows you this status update. Jane is fired later that day for disrespectful social media postings, and the two co-workers receive written warnings for their behavior.

Recent Wage and Hour Developments

- The federal Fair Labor Standards Act (FLSA) relates to:
  - Minimum wage
  - Overtime
  - Meal and rest breaks
  - Recordkeeping
- Failure to comply:
  - Back wages (for up to 3 years if willful)
  - Double damages and other penalties
  - Attorneys' fees

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

FLSA Litigation Growth

The Federal Judicial Center reports:

- 8,126 FLSA cases were filed between 4/1/2013 and 3/31/2014
  - 5% more than previous year
  - Seventh year of increases
  - Over 400% increase since 2000

Two Hot Areas

- Employees claim they have been misclassified as "exempt" and seek recovery for overtime

- Unpaid interns claim they are employees and seek recovery for all hours worked, overtime, benefits

Misclassification: Types of White Collar Exemptions

- Executive
- Administrative
- Learned Professional
- Creative Professional
- Outside Sales
- Computer Employee
- Highly Compensated Employee
  - More information available at: http://www.dol.gov/whd/regs/compliance/fairpay/fs17a_overview.pdf

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Example

Administrative Exemption Duties Test:

- The employee's primary duty must be the performance of office or non-manual work directly related to the management or general business operations of the employer or the employer's customers; and
- The employee's primary duty includes the exercise of **discretion** and **independent judgment** with respect to **matters of significance**.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Misclassification – Minimize Risk

- Confirm current job duties meet tests for exempt status
- Confirm that position performs primarily exempt duties
- Confirm that job descriptions reflect exempt status

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Unpaid Interns

There are very limited circumstances where an intern can be "unpaid" and therefore not be covered by the FLSA.

Generally, employers must satisfy all of the following criteria prior to classifying an intern as unpaid:

- The internship must be similar to training that would be given in an academic or vocational education environment, even though the internship includes actual employer operations.
- The internship must be for the intern's benefit.
- Regular employees must not be displaced by interns. Instead, the intern must work under the close supervision of existing staff.
- The employer must derive no immediate advantage from interns, and on occasion, its operations may actually be impeded by the intern.
- The intern is not necessarily entitled to a job at the end of the internship program.
- All parties must understand that the intern is not entitled to wages for any time spent in the internship program.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Unpaid Interns – Minimize Risk

- Postings/information must not suggest internship will lead to a job
- Provide letter highlighting educational opportunities of internship and unpaid status
- Intern must not replace regular staff
- Develop internship program and verify academic credit, if applicable

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

National Labor Relations Board Update

- *National Labor Relations Board v. Noel Canning*

- Continued scrutiny of overly broad employment policies

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

National Labor Relations Board v. Noel Canning

On June 26, 2014, the Supreme Court ruled:

- January 9, 2012 recess appointments of three members to the NLRB were unconstitutional because they were not made when the Senate was in a recess within the meaning of the Constitution. Rather, appointments were made when Senate was in a short recess, which lasted only three days.
- Recess appointment power applies to any recess of sufficient length, which the Supreme Court indicated typically is a recess of at least 10 days

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

National Labor Relations Board v. Noel Canning

Effect of Ruling:

- Hundreds of NLRB decisions from Jan. 9, 2012 to Aug. 5, 2013 (when the Senate confirmed a second batch of nominees for these three positions) are likely invalid – for now.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

National Labor Relations Board v. Noel Canning

Key Decisions Invalidated:

- *Banner Health Systems*: Restricted the ability to require employee confidentiality during internal investigations.
- *Sodexo America LLC*, and *Marriott International Inc.*: Expanded the rights of off-duty employees to access employer property.
- A series of decisions restricting employer ability to regulate employee use of social media, even where sharply critical of an employer or individual managers.

The NLRB likely will review and reinstate most of those decisions.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Other Recent NLRB Activity

NLRB invalidating broad provisions in confidentiality, code of conduct, and social media policies that:

"*could reasonably be interpreted as restricting the exercise of the employees' Section 7 rights under the NLRA*."

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Examples of language struck down by NLRB

-”No employee is permitted to share Confidential Information outside the organization, or to remove or make copies of any records, reports or documents in any form, without prior management approval.” Where “Confidential Information” includes “personnel information”

-Conduct rules that prohibit “disrespectful conduct,” “negative conversations,” and “derogatory attacks”

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Managing risks of NLRA-related claims

- Regularly review employment policies for compliance with updates in the law
- Prior to taking adverse employment action against any employee in response to any activity, social media, or otherwise, ask:
  - Is the employee conduct protected?
  - Is the employer consistently enforcing its social media policy in a fair, non-discriminatory, and consistent way?
  - Is the employer taking adverse action against the employee soon after the employee has engaged in other protected activity?

Bring Your Own Device – Or Bring Your Own Disaster

A 2013 Cisco study found:

- 90% of Americans use their own smart phones for work purposes.
- 40% don't password protect their smart phones
- 51% of Americans connect to unsecured wireless networks on their smartphone

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Bring Your Own Device – Important Considerations

- Protecting your data and network.
- Addressing privacy concerns.
- Employee conduct.
- Wage and hour issues.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Bring Your Own Device – Avoiding Disaster

Important guidelines for managing employees who BYOD:

1. Employees must use approved and known device. Employees must keep antivirus software up to date.

2. Device should be password protected and passwords must meet IT requirements (complexity/rotation).

3. Devices with employer information should only be used by employee.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Bring Your Own Device – Avoiding Disaster

Important guidelines for managing employees who BYOD:

- Employee must notify employer/IT right away if device compromised, lost or stolen.

- Employers should obtain signed authorization from employee in advance allowing employer to access, monitor work-related use on the device and to wipe the device in the event of a breach, loss, separation from employment or other legitimate reason.

- Non-exempt employees must record all time spent working, including time spent working on the device during nonworking hours. Policy should specify whether employees are permitted to work outside of scheduled hours without prior authorization.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Bring Your Own Device – Avoiding Disaster

Important guidelines for managing employees who BYOD:

7. Employees must comply with company policies, HIPAA and other laws and regulations in use of device.

8. Specify terms related to usage costs.

9. Detail these terms of use in a written policy.

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Questions?

aclauss@primmer.com
acramer@primmer.com
shart@primmer.com

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC

Resources

- **US Department of Health & Human Services (HHS)**
  - Enforcement Results by Year
  - Student Immunizations
  - HIPAA Privacy Rule and Sharing Information Related to Mental Health
- **HHS and US Department of Education**
  - Joint Guidance on the Application of [FERPA] and the [HIPAA] to Student Health Records
- **HHS, Office for Civil Rights**
  - Annual Report to Congress on Breaches of Unsecured Protected Health information, For Calendar Years 2011 and 2012
- ***HealthIT.gov***
  - Security Risk Assessment

2014 Legal Updates

2014 PCC Users Conference
July 18, 2014

Alexa H. Clauss, Esq.
Anne E. Cramer, Esq.
Shireen T. Hart, Esq.

Primmer Piper Eggleston & Cramer PC

www.primmer.com

PRIMMER
PRIMMER PIPER EGGLESTON & CRAMER PC