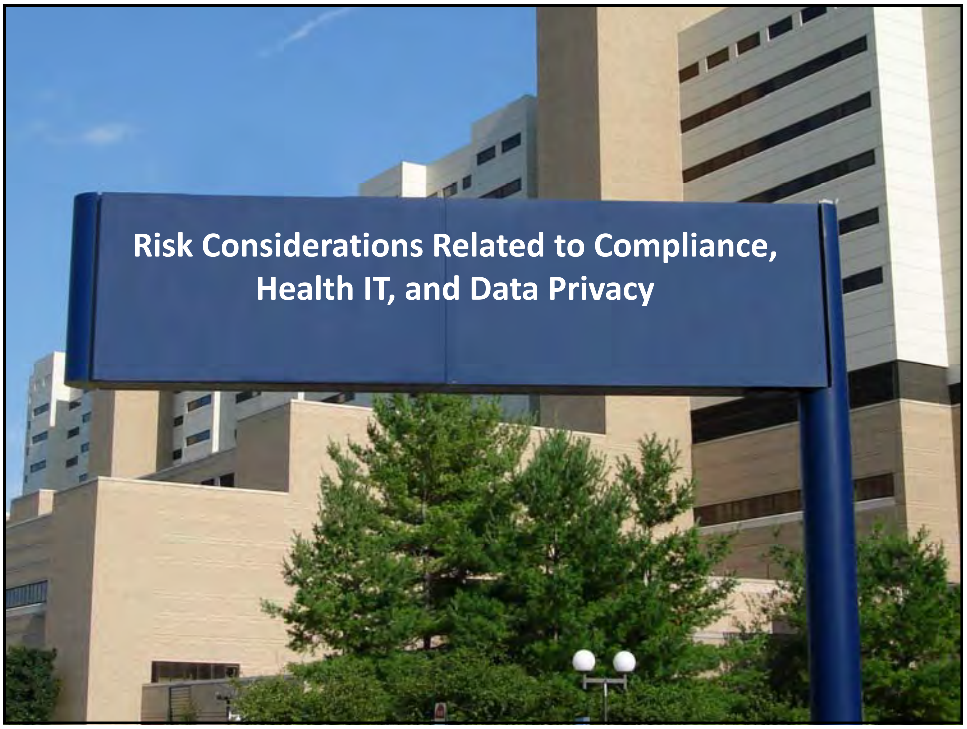
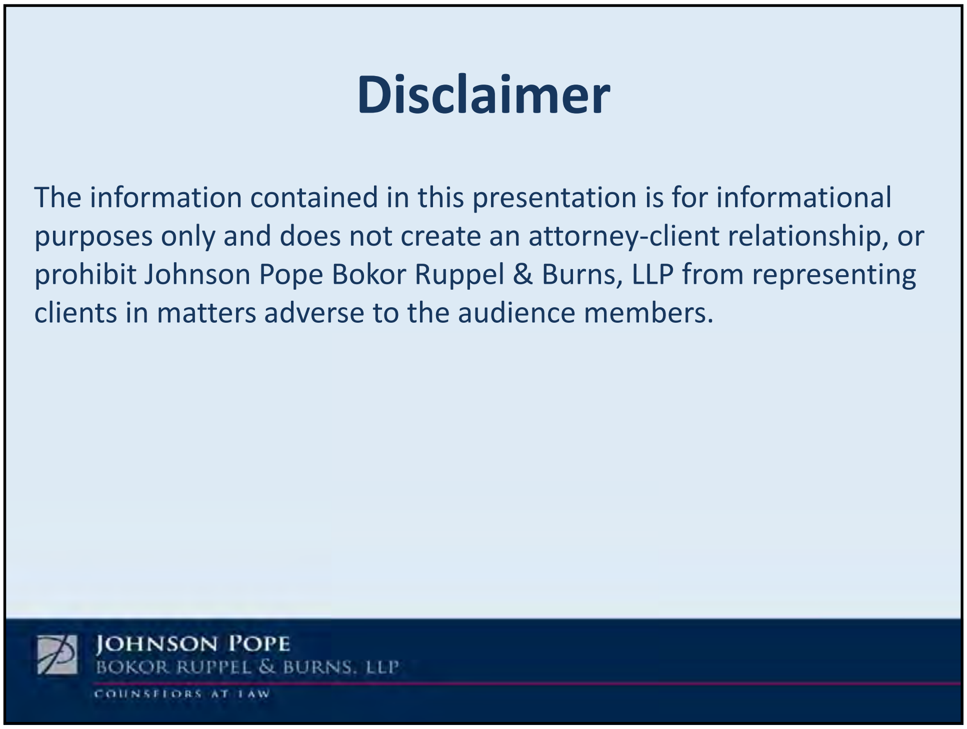
JOHNSON
POPE
BOKOR
RUPPEL &
BURNS, LLP

COUNSELORS AT LAW



# Risk Considerations Related to Compliance, Health IT, and Data Privacy



# Disclaimer

The information contained in this presentation is for informational purposes only and does not create an attorney-client relationship, or prohibit Johnson Pope Bokor Ruppel & Burns, LLP from representing clients in matters adverse to the audience members.

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

# Topics

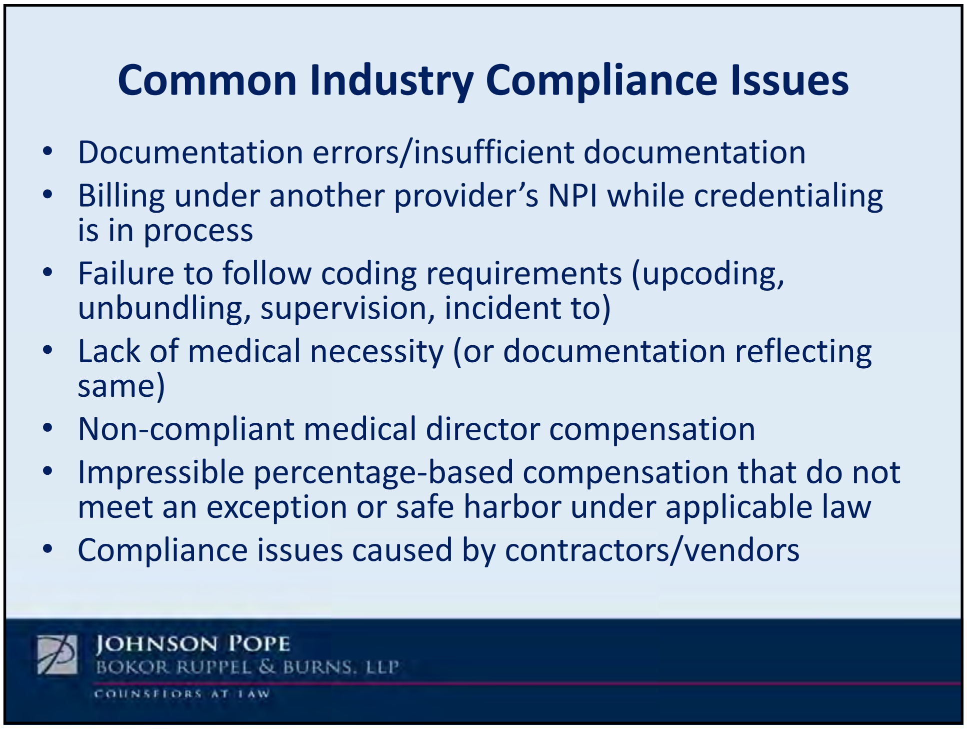
- Compliance programs & how they can help manage risks
- Risks related to health IT & contracts
- Data privacy, security, and HIPAA briefing

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

## Why does compliance matter?

- Failure to comply creates risk!
- Penalties and fines
- Criminal prosecution
- Licensure actions
- Patient trust
- Reputational harm
- Lawsuits $$$

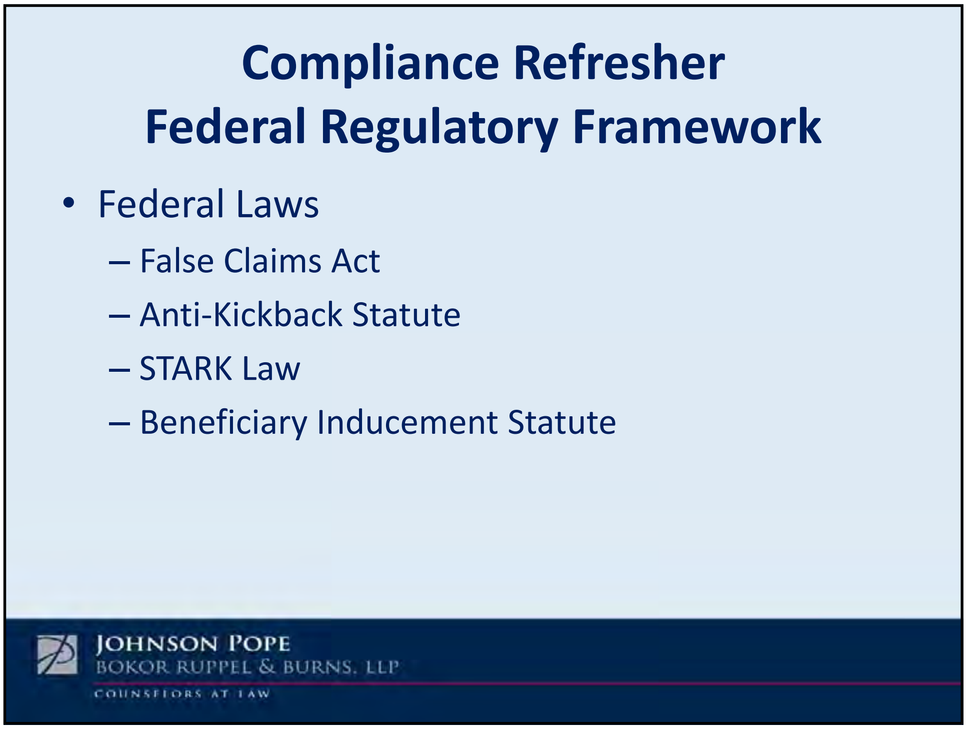
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



## Common Industry Compliance Issues

- Documentation errors/insufficient documentation
- Billing under another provider's NPI while credentialing is in process
- Failure to follow coding requirements (upcoding, unbundling, supervision, incident to)
- Lack of medical necessity (or documentation reflecting same)
- Non-compliant medical director compensation
- Impressible percentage-based compensation that do not meet an exception or safe harbor under applicable law
- Compliance issues caused by contractors/vendors

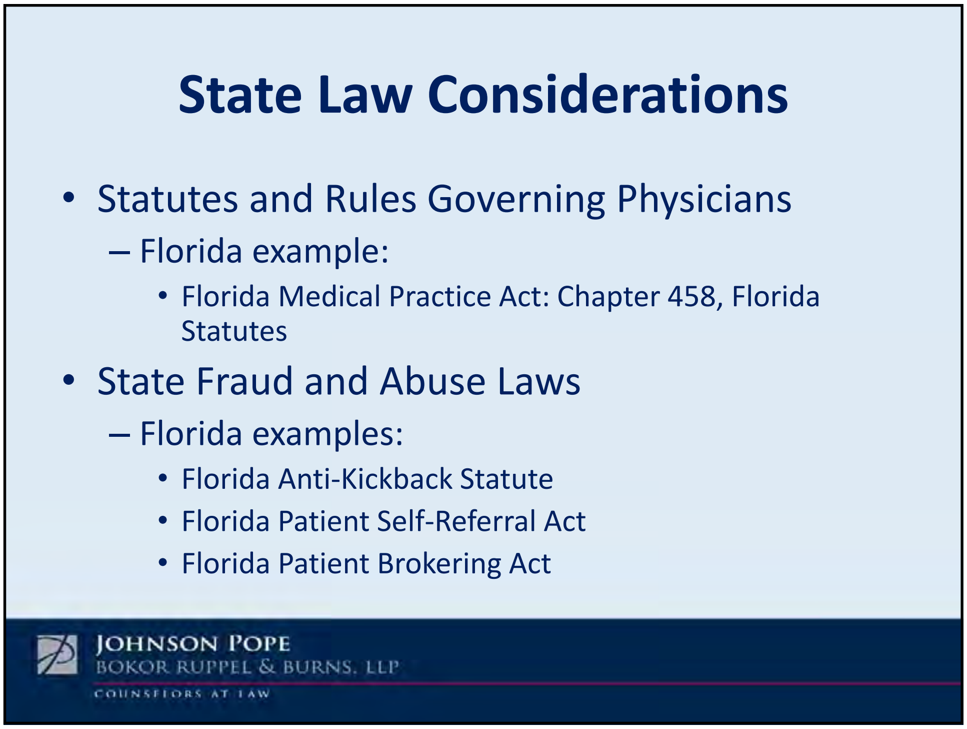
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Compliance Refresher
# Federal Regulatory Framework

- Federal Laws
  - False Claims Act
  - Anti-Kickback Statute
  - STARK Law
  - Beneficiary Inducement Statute

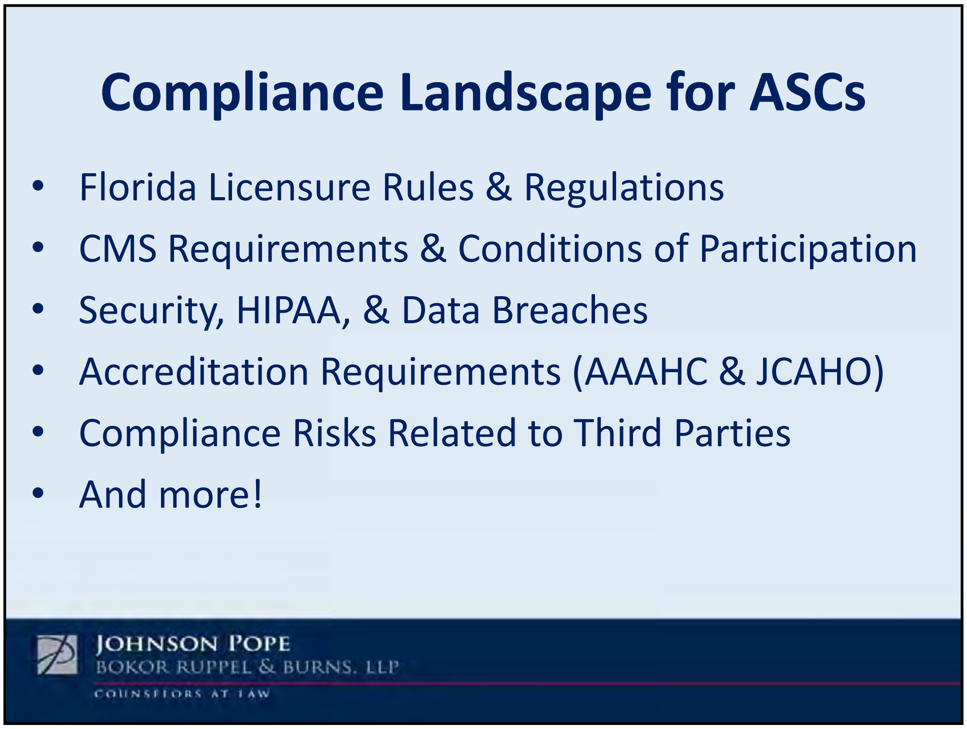
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# State Law Considerations

- Statutes and Rules Governing Physicians
  - Florida example:
    - Florida Medical Practice Act: Chapter 458, Florida Statutes
- State Fraud and Abuse Laws
  - Florida examples:
    - Florida Anti-Kickback Statute
    - Florida Patient Self-Referral Act
    - Florida Patient Brokering Act

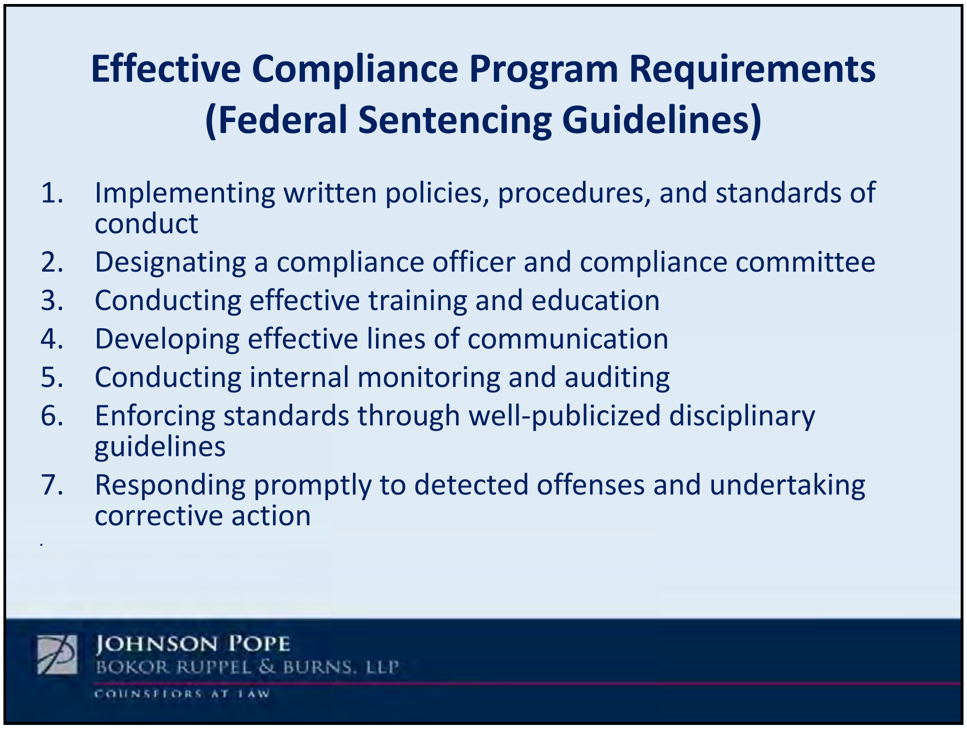
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



## Compliance Landscape for ASCs

- Florida Licensure Rules & Regulations
- CMS Requirements & Conditions of Participation
- Security, HIPAA, & Data Breaches
- Accreditation Requirements (AAAHC & JCAHO)
- Compliance Risks Related to Third Parties
- And more!

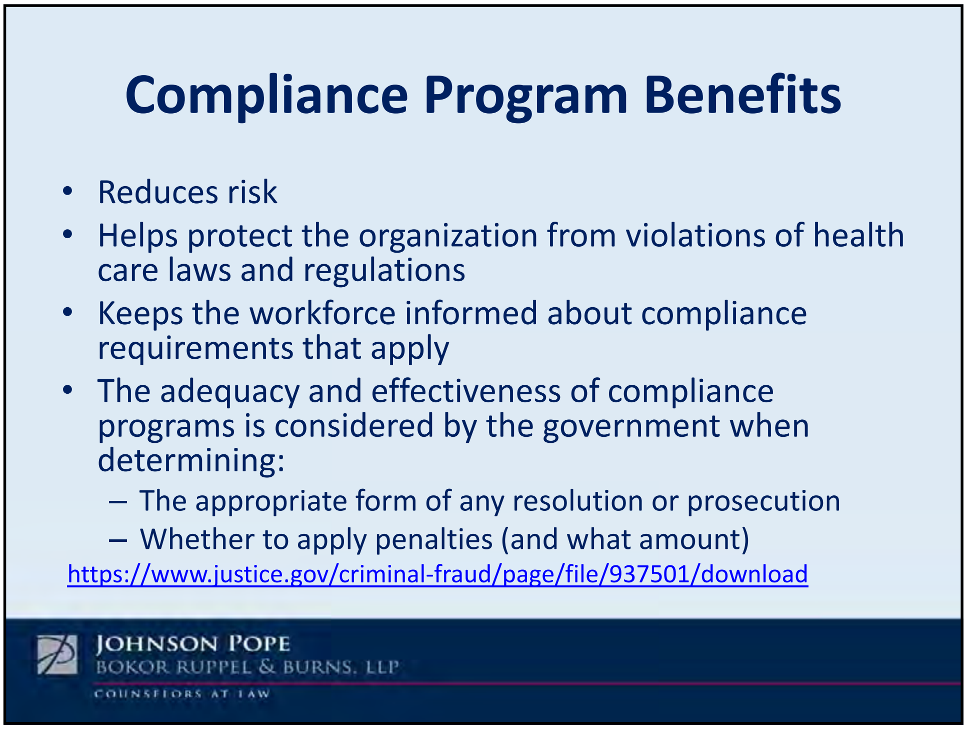
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



## Effective Compliance Program Requirements (Federal Sentencing Guidelines)

1. Implementing written policies, procedures, and standards of conduct
2. Designating a compliance officer and compliance committee
3. Conducting effective training and education
4. Developing effective lines of communication
5. Conducting internal monitoring and auditing
6. Enforcing standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective action

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

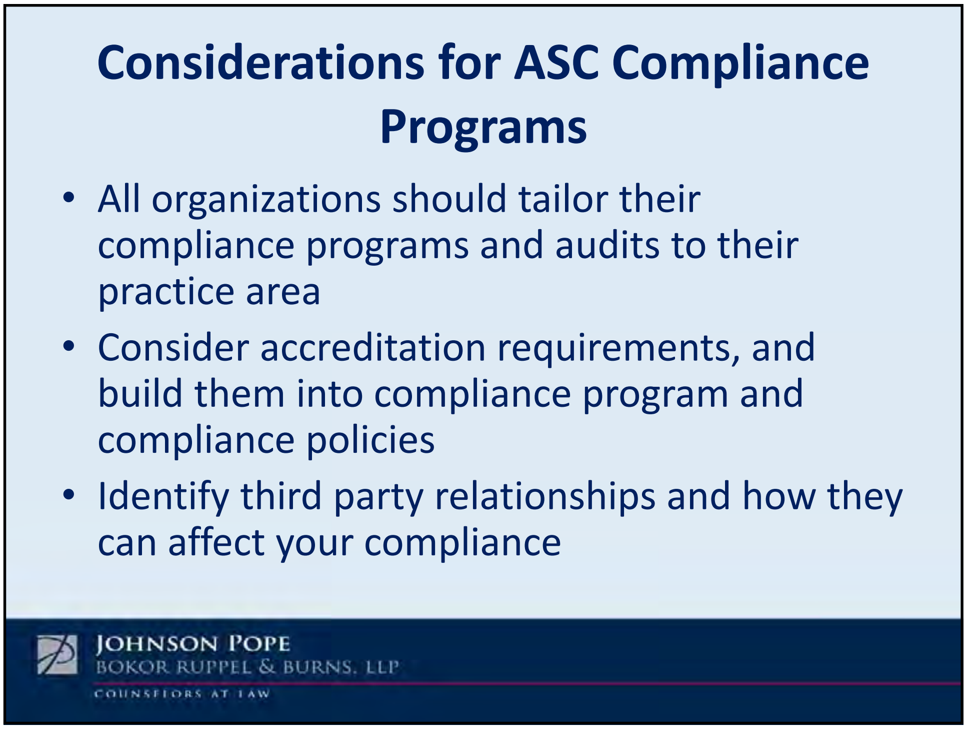


# Compliance Program Benefits

- Reduces risk
- Helps protect the organization from violations of health care laws and regulations
- Keeps the workforce informed about compliance requirements that apply
- The adequacy and effectiveness of compliance programs is considered by the government when determining:
  - The appropriate form of any resolution or prosecution
  - Whether to apply penalties (and what amount)

https://www.justice.gov/criminal-fraud/page/file/937501/download

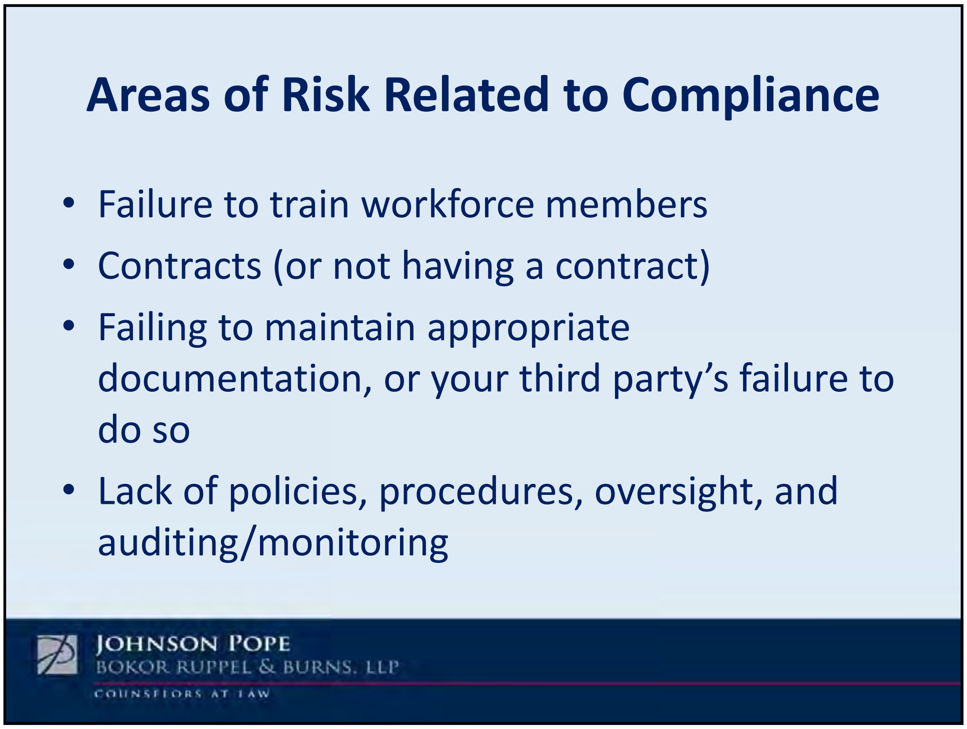
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Considerations for ASC Compliance Programs

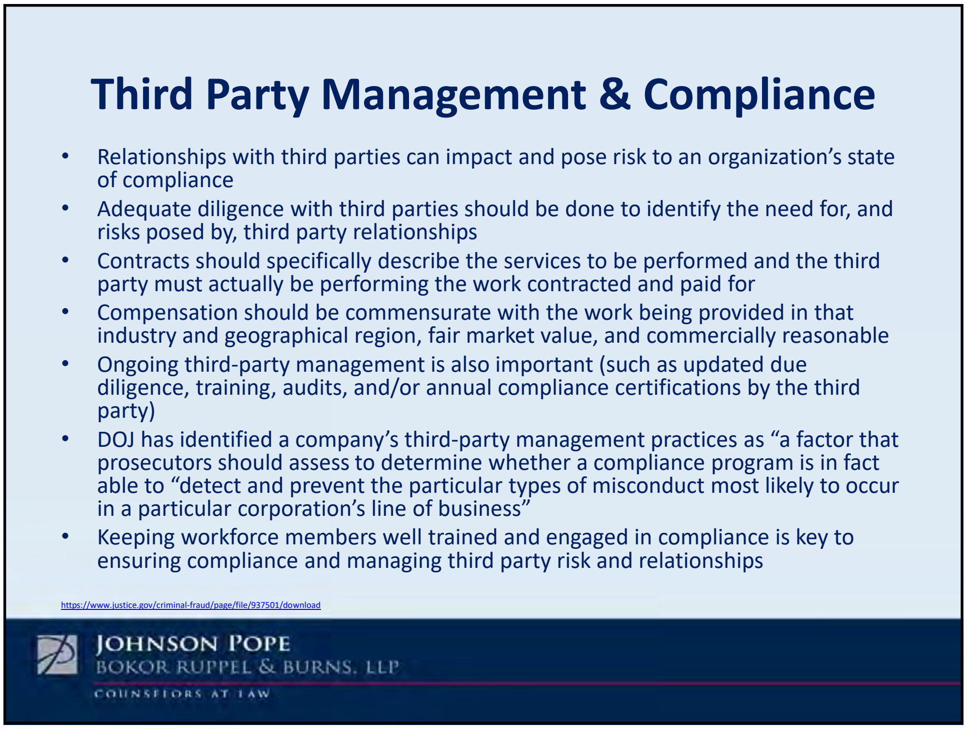
- All organizations should tailor their compliance programs and audits to their practice area
- Consider accreditation requirements, and build them into compliance program and compliance policies
- Identify third party relationships and how they can affect your compliance

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Areas of Risk Related to Compliance

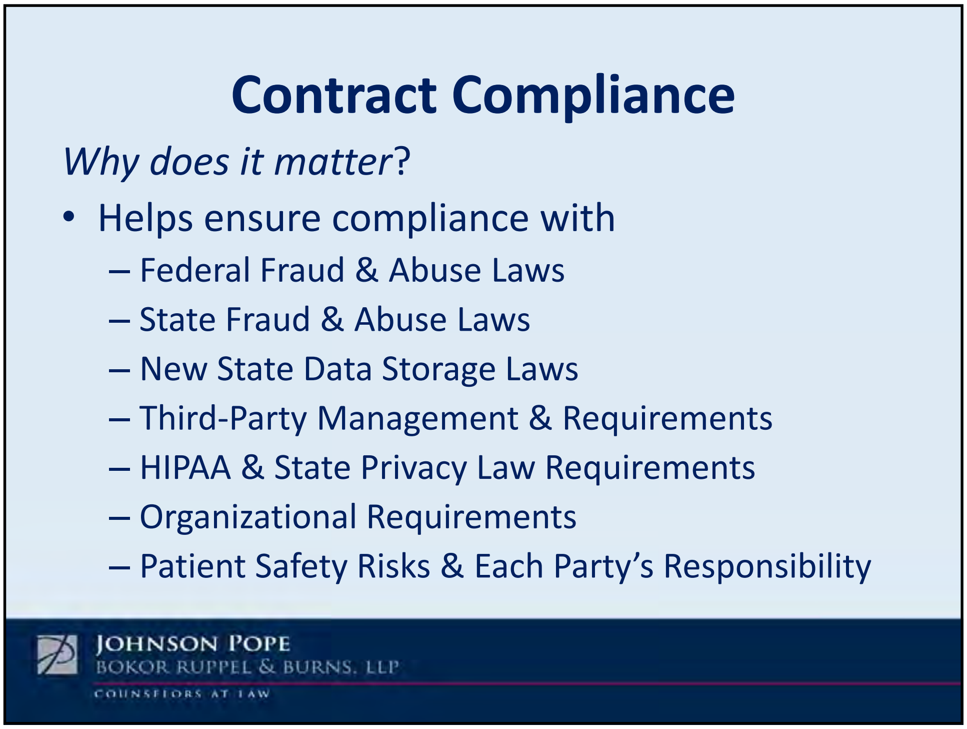
- Failure to train workforce members
- Contracts (or not having a contract)
- Failing to maintain appropriate documentation, or your third party's failure to do so
- Lack of policies, procedures, oversight, and auditing/monitoring



# Third Party Management & Compliance

- Relationships with third parties can impact and pose risk to an organization's state of compliance
- Adequate diligence with third parties should be done to identify the need for, and risks posed by, third party relationships
- Contracts should specifically describe the services to be performed and the third party must actually be performing the work contracted and paid for
- Compensation should be commensurate with the work being provided in that industry and geographical region, fair market value, and commercially reasonable
- Ongoing third-party management is also important (such as updated due diligence, training, audits, and/or annual compliance certifications by the third party)
- DOJ has identified a company's third-party management practices as "a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect and prevent the particular types of misconduct most likely to occur in a particular corporation's line of business"
- Keeping workforce members well trained and engaged in compliance is key to ensuring compliance and managing third party risk and relationships

https://www.justice.gov/criminal-fraud/page/file/937501/download

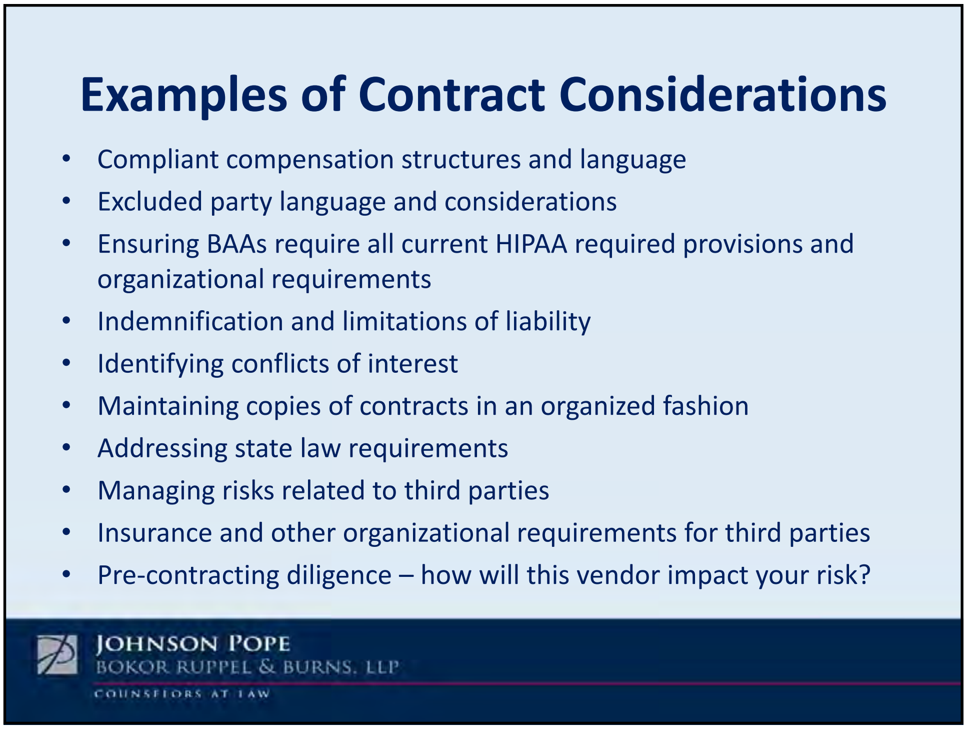


# Contract Compliance

*Why does it matter*?

- Helps ensure compliance with
  - Federal Fraud & Abuse Laws
  - State Fraud & Abuse Laws
  - New State Data Storage Laws
  - Third-Party Management & Requirements
  - HIPAA & State Privacy Law Requirements
  - Organizational Requirements
  - Patient Safety Risks & Each Party's Responsibility

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Examples of Contract Considerations

- Compliant compensation structures and language
- Excluded party language and considerations
- Ensuring BAAs require all current HIPAA required provisions and organizational requirements
- Indemnification and limitations of liability
- Identifying conflicts of interest
- Maintaining copies of contracts in an organized fashion
- Addressing state law requirements
- Managing risks related to third parties
- Insurance and other organizational requirements for third parties
- Pre-contracting diligence – how will this vendor impact your risk?

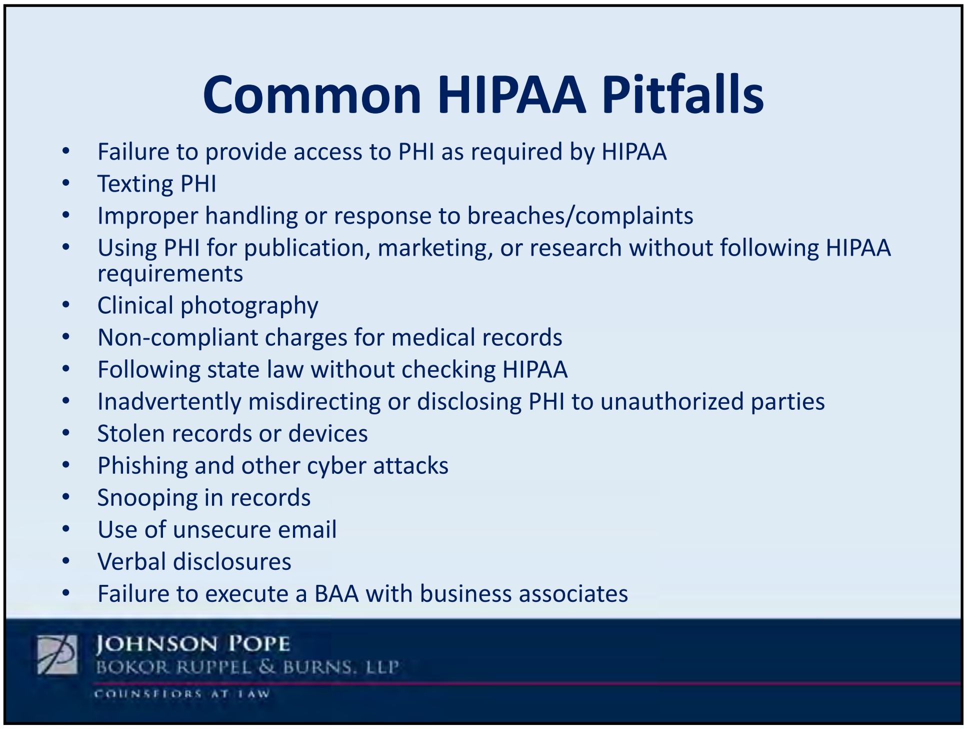
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

# The Importance of a BAA Example Press Release

- **No Business Associate Agreement? $31K Mistake – April 20, 2017**
- The Center for Children's Digestive Health (CCDH) has paid the U.S. Department of Health and Human Services (HHS) $31,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and agreed to implement a corrective action plan. CCDH is a small, for-profit health care provider with a pediatric subspecialty practice that operates its practice in seven clinic locations in Illinois.
- In August 2015, the HHS Office for Civil Rights (OCR) initiated a compliance review of the Center for Children's Digestive Health (CCDH) following an initiation of an investigation of a business associate, FileFax, Inc., which stored records containing protected health information (PHI) for CCDH. While CCDH began disclosing PHI to Filefax in 2003, neither party could produce a signed Business Associate Agreement (BAA) prior to Oct. 12, 2015.
- Read the Resolution Agreement and Corrective Action Plan - PDF
- For more information on Business Associate Agreements, please visit https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

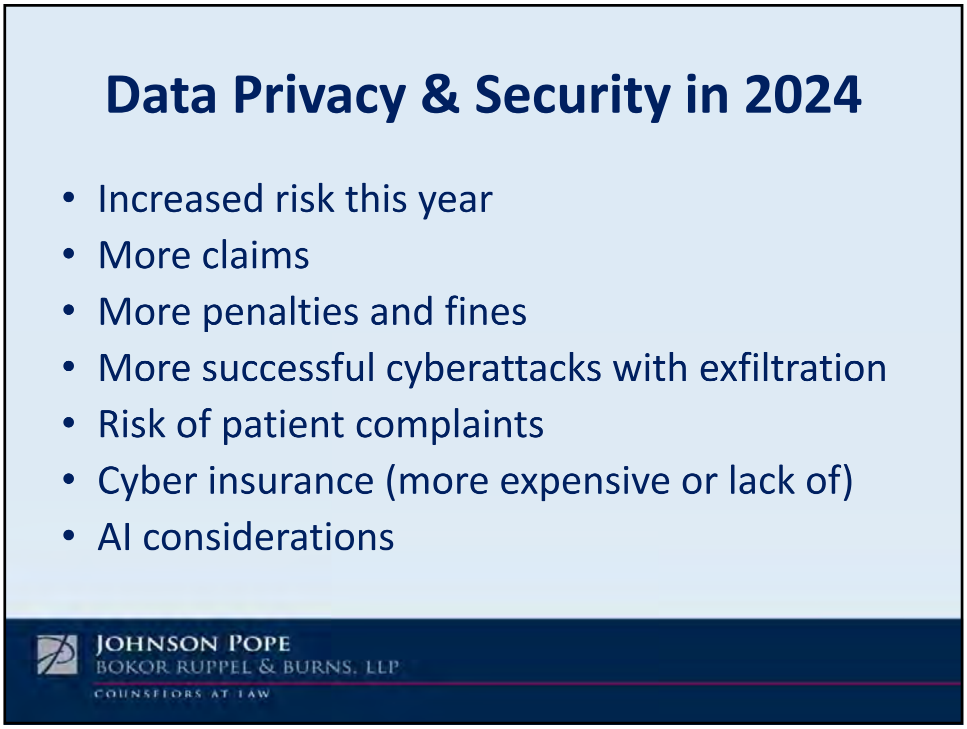
https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html

# Data Privacy & Security in 2024



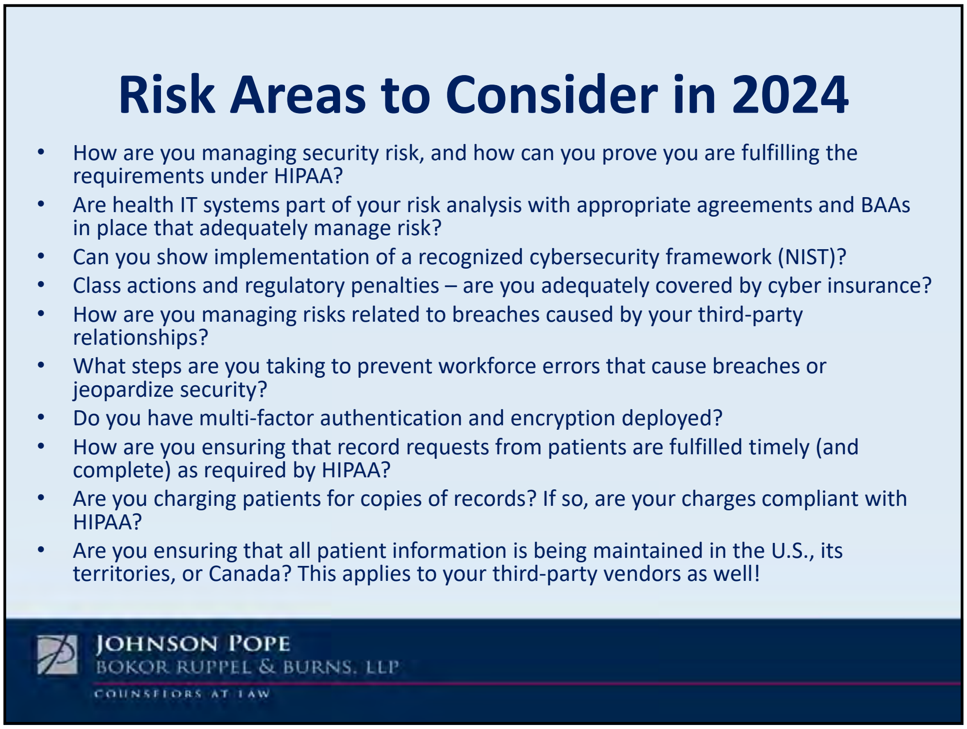
# Common HIPAA Pitfalls

- Failure to provide access to PHI as required by HIPAA
- Texting PHI
- Improper handling or response to breaches/complaints
- Using PHI for publication, marketing, or research without following HIPAA requirements
- Clinical photography
- Non-compliant charges for medical records
- Following state law without checking HIPAA
- Inadvertently misdirecting or disclosing PHI to unauthorized parties
- Stolen records or devices
- Phishing and other cyber attacks
- Snooping in records
- Use of unsecure email
- Verbal disclosures
- Failure to execute a BAA with business associates



# Data Privacy & Security in 2024

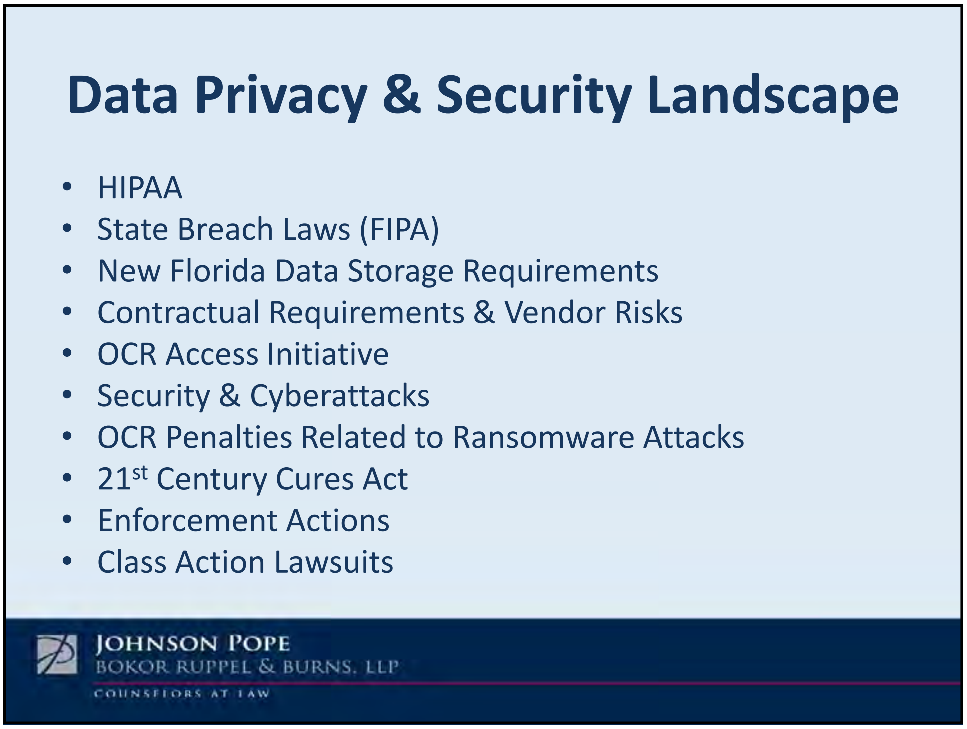
- Increased risk this year
- More claims
- More penalties and fines
- More successful cyberattacks with exfiltration
- Risk of patient complaints
- Cyber insurance (more expensive or lack of)
- AI considerations



# Risk Areas to Consider in 2024

- How are you managing security risk, and how can you prove you are fulfilling the requirements under HIPAA?
- Are health IT systems part of your risk analysis with appropriate agreements and BAAs in place that adequately manage risk?
- Can you show implementation of a recognized cybersecurity framework (NIST)?
- Class actions and regulatory penalties – are you adequately covered by cyber insurance?
- How are you managing risks related to breaches caused by your third-party relationships?
- What steps are you taking to prevent workforce errors that cause breaches or jeopardize security?
- Do you have multi-factor authentication and encryption deployed?
- How are you ensuring that record requests from patients are fulfilled timely (and complete) as required by HIPAA?
- Are you charging patients for copies of records? If so, are your charges compliant with HIPAA?
- Are you ensuring that all patient information is being maintained in the U.S., its territories, or Canada? This applies to your third-party vendors as well!

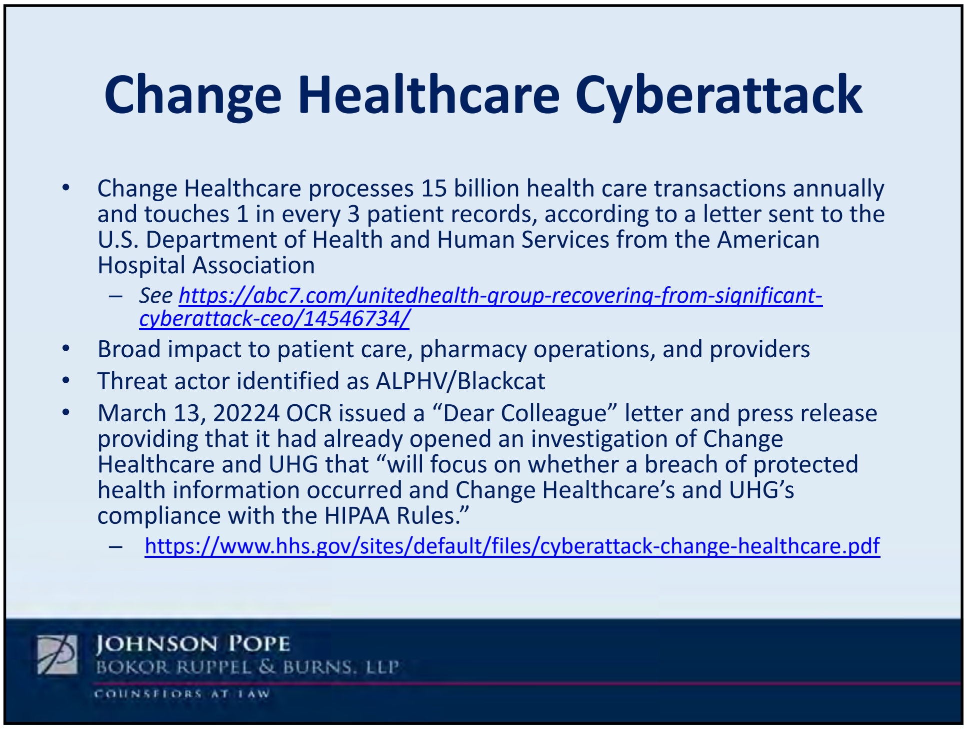
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Data Privacy & Security Landscape

- HIPAA
- State Breach Laws (FIPA)
- New Florida Data Storage Requirements
- Contractual Requirements & Vendor Risks
- OCR Access Initiative
- Security & Cyberattacks
- OCR Penalties Related to Ransomware Attacks
- 21st Century Cures Act
- Enforcement Actions
- Class Action Lawsuits

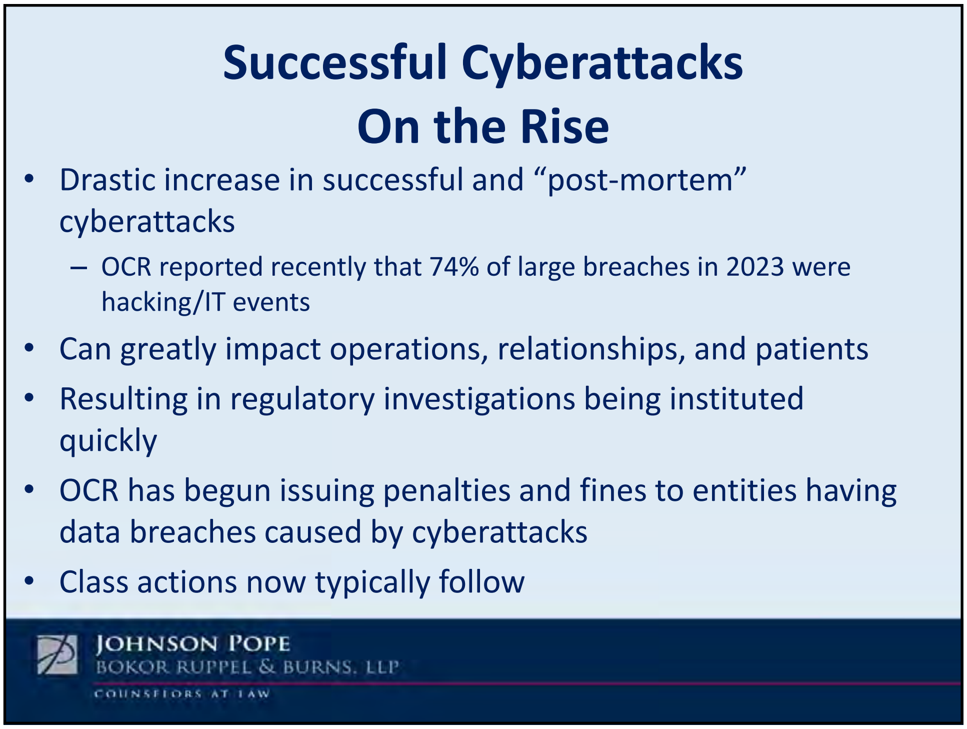
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



## Change Healthcare Cyberattack

- Change Healthcare processes 15 billion health care transactions annually and touches 1 in every 3 patient records, according to a letter sent to the U.S. Department of Health and Human Services from the American Hospital Association
  - *See https://abc7.com/unitedhealth-group-recovering-from-significant-cyberattack-ceo/14546734/*
- Broad impact to patient care, pharmacy operations, and providers
- Threat actor identified as ALPHV/Blackcat
- March 13, 20224 OCR issued a “Dear Colleague” letter and press release providing that it had already opened an investigation of Change Healthcare and UHG that “will focus on whether a breach of protected health information occurred and Change Healthcare’s and UHG’s compliance with the HIPAA Rules.”
  - https://www.hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf

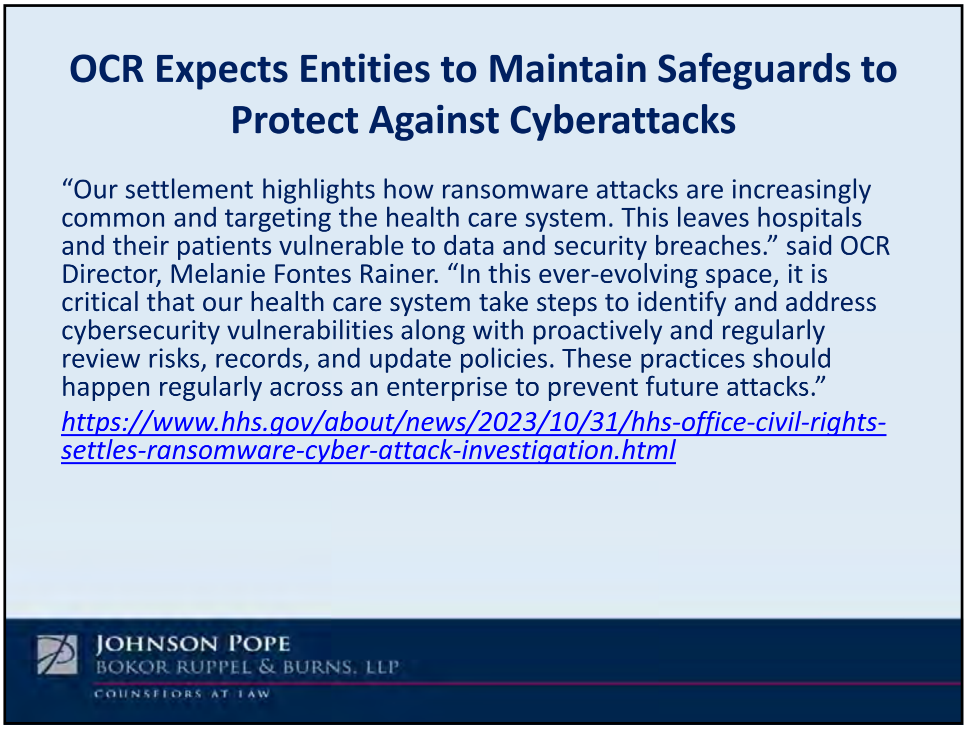
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



## Successful Cyberattacks On the Rise

- Drastic increase in successful and “post-mortem” cyberattacks
  - OCR reported recently that 74% of large breaches in 2023 were hacking/IT events
- Can greatly impact operations, relationships, and patients
- Resulting in regulatory investigations being instituted quickly
- OCR has begun issuing penalties and fines to entities having data breaches caused by cyberattacks
- Class actions now typically follow

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

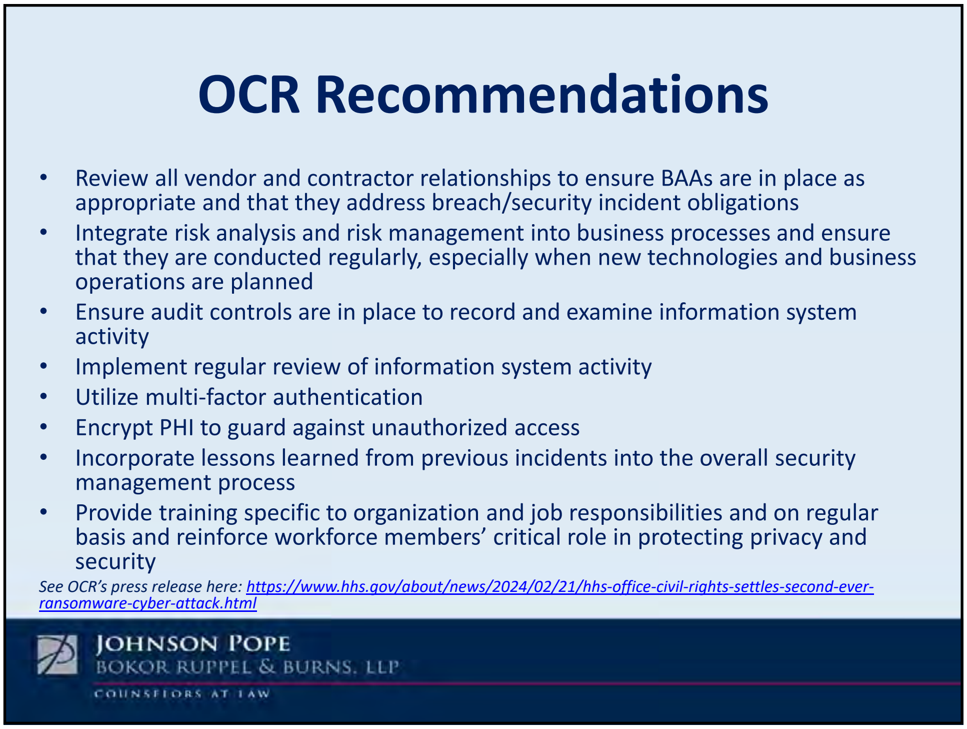


## OCR Expects Entities to Maintain Safeguards to Protect Against Cyberattacks

"Our settlement highlights how ransomware attacks are increasingly common and targeting the health care system. This leaves hospitals and their patients vulnerable to data and security breaches." said OCR Director, Melanie Fontes Rainer. "In this ever-evolving space, it is critical that our health care system take steps to identify and address cybersecurity vulnerabilities along with proactively and regularly review risks, records, and update policies. These practices should happen regularly across an enterprise to prevent future attacks."

*https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html*

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

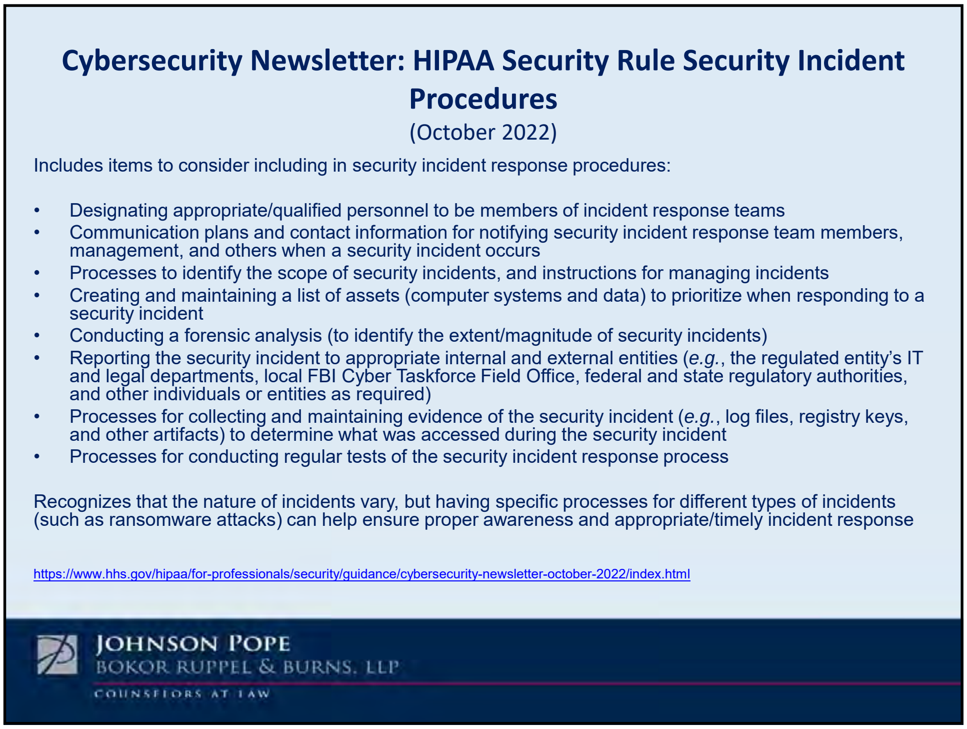


## OCR Recommendations

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and that they address breach/security incident obligations
- Integrate risk analysis and risk management into business processes and ensure that they are conducted regularly, especially when new technologies and business operations are planned
- Ensure audit controls are in place to record and examine information system activity
- Implement regular review of information system activity
- Utilize multi-factor authentication
- Encrypt PHI to guard against unauthorized access
- Incorporate lessons learned from previous incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis and reinforce workforce members' critical role in protecting privacy and security

*See OCR's press release here: https://www.hhs.gov/about/news/2024/02/21/hhs-office-civil-rights-settles-second-ever-ransomware-cyber-attack.html*

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



## Cybersecurity Newsletter: HIPAA Security Rule Security Incident Procedures

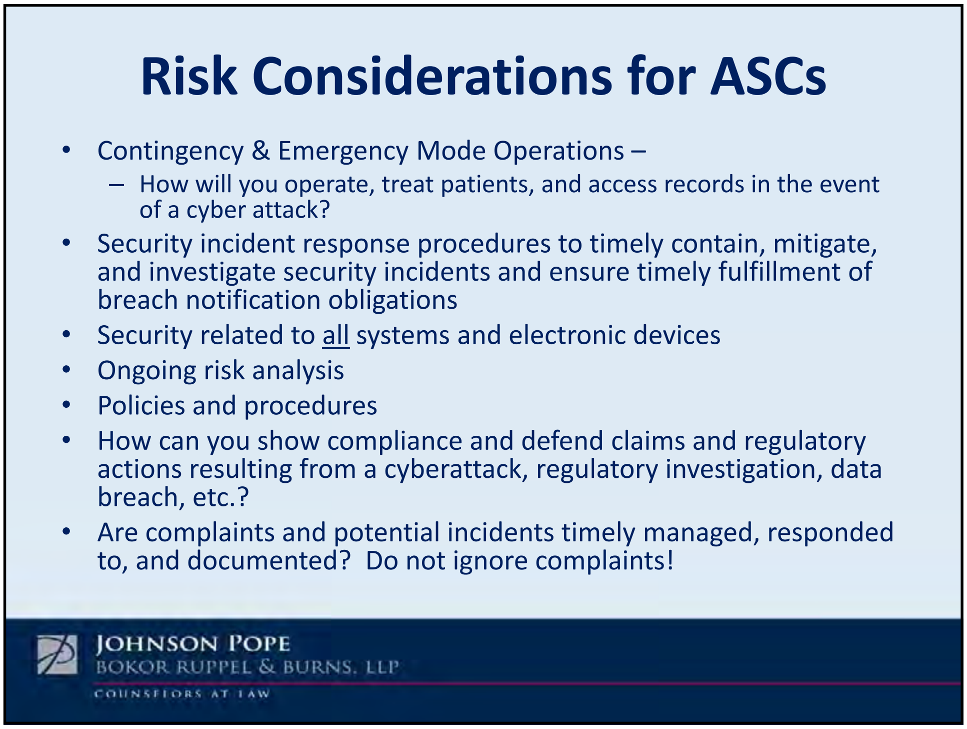
(October 2022)

Includes items to consider including in security incident response procedures:

- Designating appropriate/qualified personnel to be members of incident response teams
- Communication plans and contact information for notifying security incident response team members, management, and others when a security incident occurs
- Processes to identify the scope of security incidents, and instructions for managing incidents
- Creating and maintaining a list of assets (computer systems and data) to prioritize when responding to a security incident
- Conducting a forensic analysis (to identify the extent/magnitude of security incidents)
- Reporting the security incident to appropriate internal and external entities (*e.g.*, the regulated entity's IT and legal departments, local FBI Cyber Taskforce Field Office, federal and state regulatory authorities, and other individuals or entities as required)
- Processes for collecting and maintaining evidence of the security incident (*e.g.*, log files, registry keys, and other artifacts) to determine what was accessed during the security incident
- Processes for conducting regular tests of the security incident response process

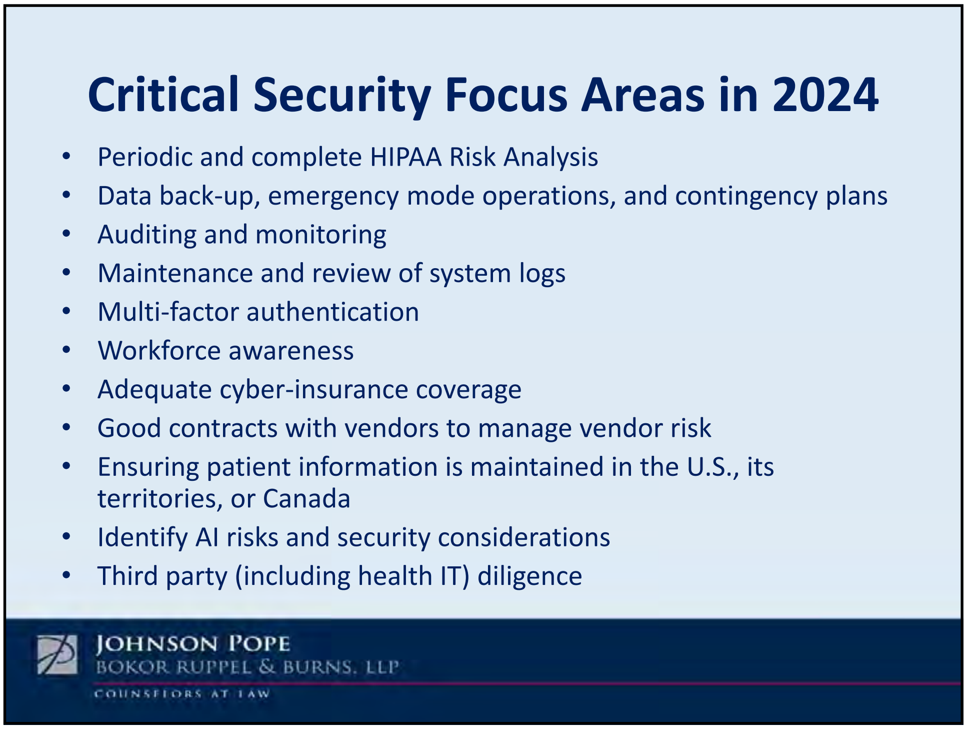
Recognizes that the nature of incidents vary, but having specific processes for different types of incidents (such as ransomware attacks) can help ensure proper awareness and appropriate/timely incident response

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2022/index.html



## Risk Considerations for ASCs

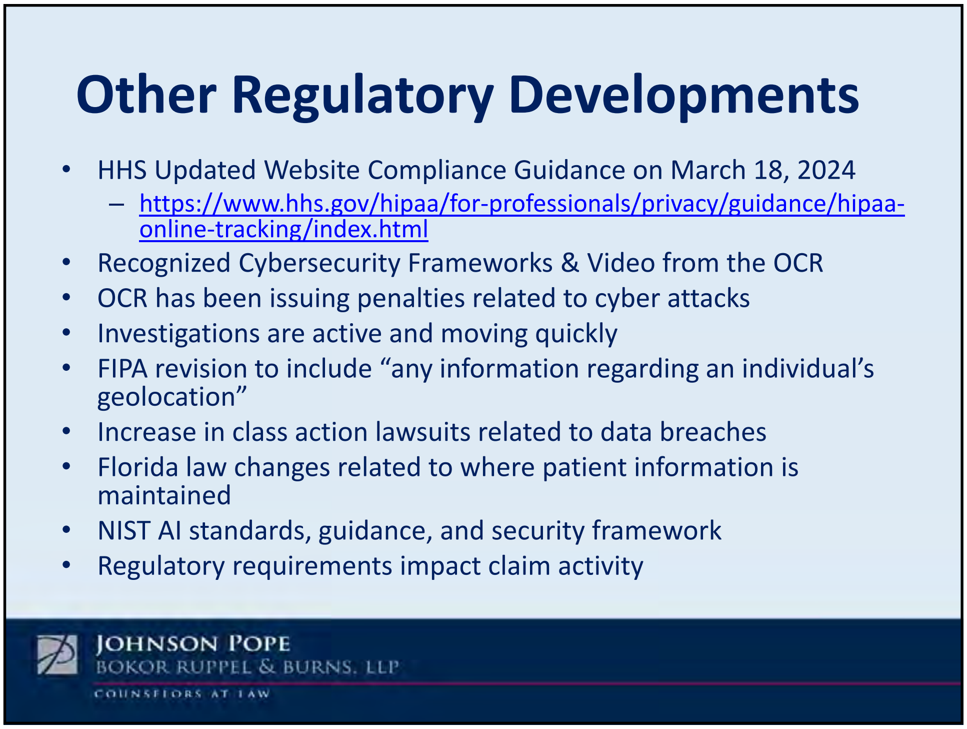
- Contingency & Emergency Mode Operations –
  - How will you operate, treat patients, and access records in the event of a cyber attack?
- Security incident response procedures to timely contain, mitigate, and investigate security incidents and ensure timely fulfillment of breach notification obligations
- Security related to all systems and electronic devices
- Ongoing risk analysis
- Policies and procedures
- How can you show compliance and defend claims and regulatory actions resulting from a cyberattack, regulatory investigation, data breach, etc.?
- Are complaints and potential incidents timely managed, responded to, and documented? Do not ignore complaints!



# Critical Security Focus Areas in 2024

- Periodic and complete HIPAA Risk Analysis
- Data back-up, emergency mode operations, and contingency plans
- Auditing and monitoring
- Maintenance and review of system logs
- Multi-factor authentication
- Workforce awareness
- Adequate cyber-insurance coverage
- Good contracts with vendors to manage vendor risk
- Ensuring patient information is maintained in the U.S., its territories, or Canada
- Identify AI risks and security considerations
- Third party (including health IT) diligence

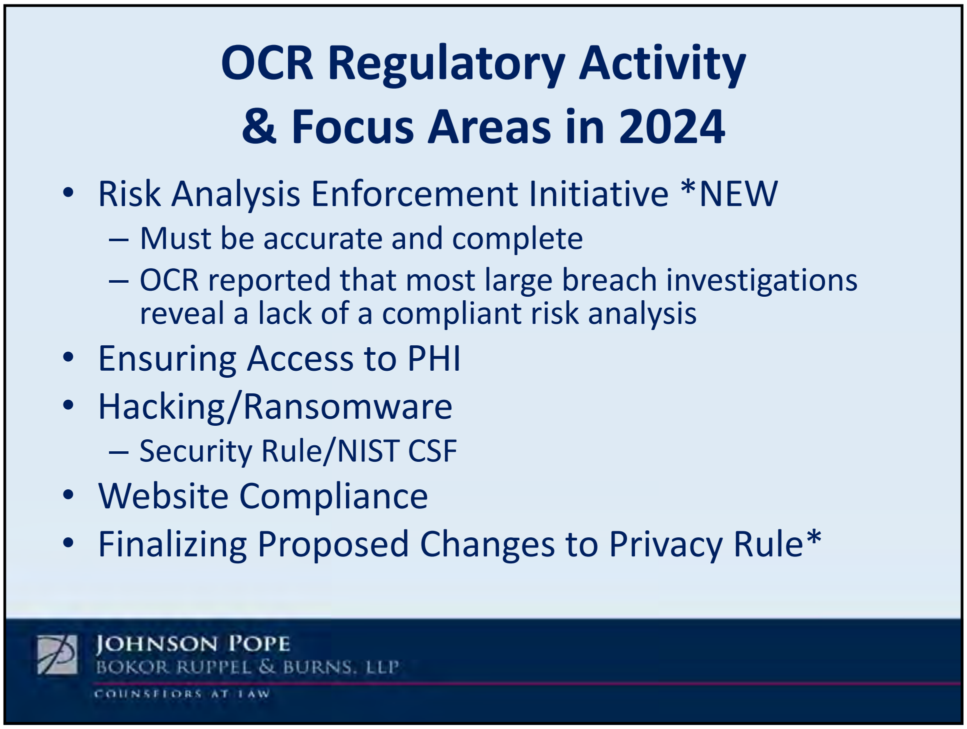
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Other Regulatory Developments

- HHS Updated Website Compliance Guidance on March 18, 2024
  - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
- Recognized Cybersecurity Frameworks & Video from the OCR
- OCR has been issuing penalties related to cyber attacks
- Investigations are active and moving quickly
- FIPA revision to include “any information regarding an individual’s geolocation”
- Increase in class action lawsuits related to data breaches
- Florida law changes related to where patient information is maintained
- NIST AI standards, guidance, and security framework
- Regulatory requirements impact claim activity

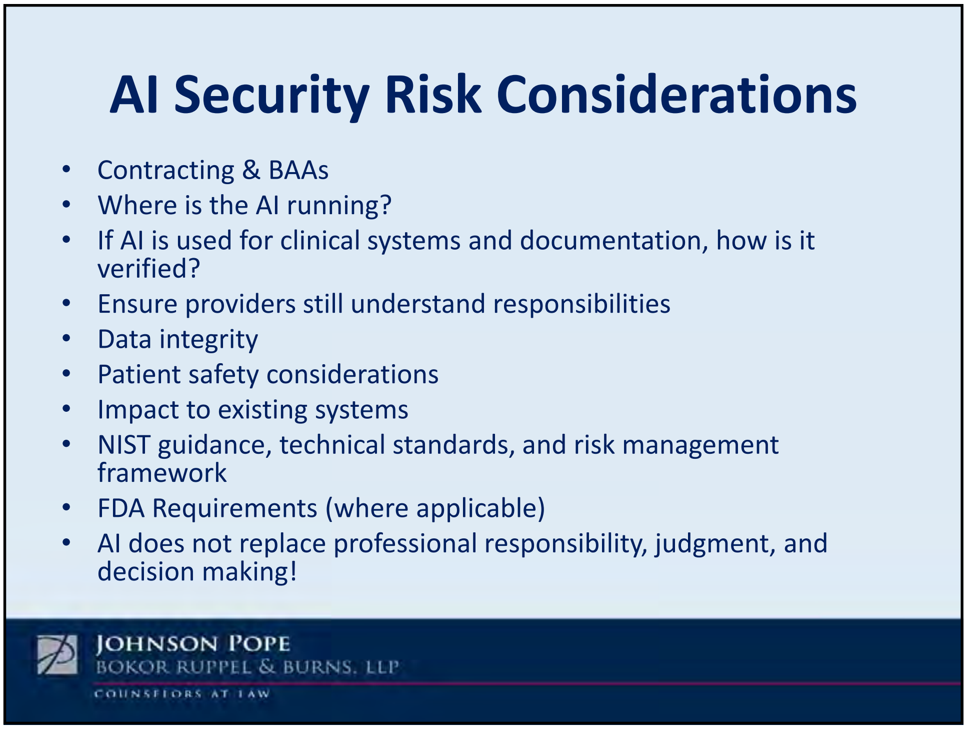
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# OCR Regulatory Activity & Focus Areas in 2024

- Risk Analysis Enforcement Initiative *NEW
  - Must be accurate and complete
  - OCR reported that most large breach investigations reveal a lack of a compliant risk analysis
- Ensuring Access to PHI
- Hacking/Ransomware
  - Security Rule/NIST CSF
- Website Compliance
- Finalizing Proposed Changes to Privacy Rule*

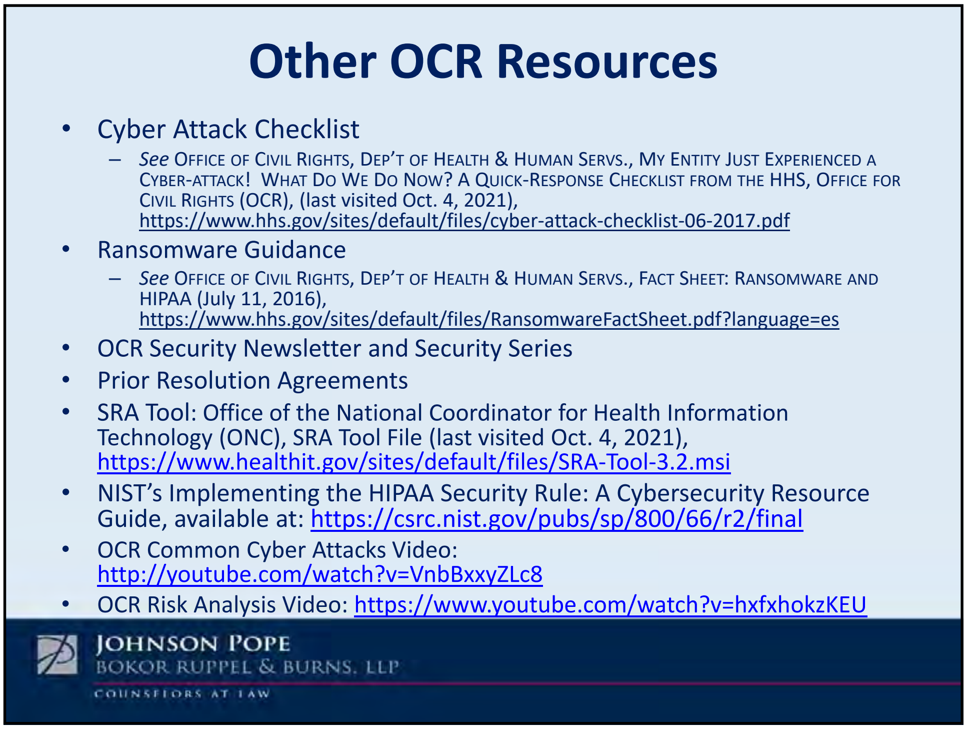
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# AI Security Risk Considerations

- Contracting & BAAs
- Where is the AI running?
- If AI is used for clinical systems and documentation, how is it verified?
- Ensure providers still understand responsibilities
- Data integrity
- Patient safety considerations
- Impact to existing systems
- NIST guidance, technical standards, and risk management framework
- FDA Requirements (where applicable)
- AI does not replace professional responsibility, judgment, and decision making!

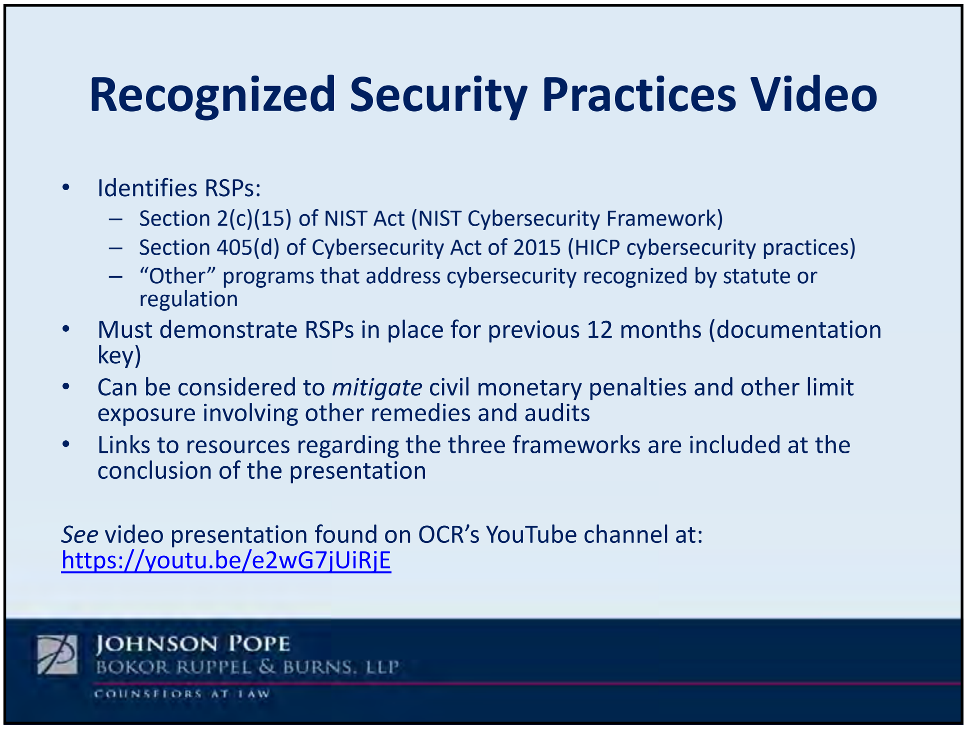
JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Other OCR Resources

- Cyber Attack Checklist
  - *See* Office of Civil Rights, Dep't of Health & Human Servs., My Entity Just Experienced a Cyber-attack! What Do We Do Now? A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR), (last visited Oct. 4, 2021), https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf
- Ransomware Guidance
  - *See* Office of Civil Rights, Dep't of Health & Human Servs., Fact Sheet: Ransomware and HIPAA (July 11, 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es
- OCR Security Newsletter and Security Series
- Prior Resolution Agreements
- SRA Tool: Office of the National Coordinator for Health Information Technology (ONC), SRA Tool File (last visited Oct. 4, 2021), https://www.healthit.gov/sites/default/files/SRA-Tool-3.2.msi
- NIST's Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide, available at: https://csrc.nist.gov/pubs/sp/800/66/r2/final
- OCR Common Cyber Attacks Video: http://youtube.com/watch?v=VnbBxxyZLc8
- OCR Risk Analysis Video: https://www.youtube.com/watch?v=hxfxhokzKEU

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW



# Recognized Security Practices Video

- Identifies RSPs:
  - Section 2(c)(15) of NIST Act (NIST Cybersecurity Framework)
  - Section 405(d) of Cybersecurity Act of 2015 (HICP cybersecurity practices)
  - "Other" programs that address cybersecurity recognized by statute or regulation
- Must demonstrate RSPs in place for previous 12 months (documentation key)
- Can be considered to *mitigate* civil monetary penalties and other limit exposure involving other remedies and audits
- Links to resources regarding the three frameworks are included at the conclusion of the presentation

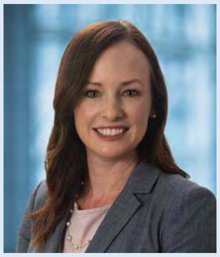
*See* video presentation found on OCR's YouTube channel at: https://youtu.be/e2wG7jUiRjE

JOHNSON POPE
BOKOR RUPPEL & BURNS, LLP
COUNSELORS AT LAW

## Recognized Security Practices Video

- Adopting recognized cybersecurity framework is still voluntary
- Entities under investigation or selected for an audit may be invited to submit data/information related to implemented recognized cybersecurity frameworks (data request)
- The data request may include examples of the type of evidence that may be provided
- Show actively in use (and for past 12 months) and fully implemented throughout the organization

*See* video presentation found on OCR's YouTube channel at: https://youtu.be/e2wG7jUiRjE



Joy S. Easterwood, Esq., CHPC

813-225-2500

joye@jpfirm.com

www.jpfirm.com