

Hot Button Labor and Ops Issues

... trends that have our attention.

Agenda

- 1) Dealing with Regulatory Investigations
- 2) Handling Press Inquiries/Preparing for Crisis Communications
- 3) New NH Privacy Law
- 4) Private Equity Funding Litigation
- 5) Whistleblowers



Dealing with Regulatory Investigations

Bradley D. Holt, Esquire
(mostly healthcare litigation)



Uh oh: you're under investigation by a regulatory body!

- NH Office of Professional Licensure & Certification (OPLC)
- ME Office of Professional and Occupational Regulation (OPOR)
- Attorney General's Office

The Legal Landscape (NH)

- OPLC initiated about 5 years ago

Initial proposal:

“The purpose of the Office of Professional Licensure and Certification (OPLC) is to **promote efficient professional healthcare licensing** and professional technical licensing in the State of New Hampshire. The **OPLC oversees the administration** of forty-seven occupational licensing boards; **these Boards**, Councils, and Commissions directly **regulate their professions** pursuant to the powers, duties, functions, and responsibilities granted to them by individual practice acts. **OPLC provides administrative, clerical, business processing and recordkeeping support to these Boards...**”

A trend:

Unprecedented discretion to the OPLC investigatory and prosecuting teams:

- aggressive investigation and recommendations to Boards
 - “Hobson’s Choice”
 - To overturn a bad recommendation requires prevailing at a public hearing

The boards that matter to Senior Living providers

Of the 50+ boards:

- Board of Nursing
- Board of Barbering, Cosmetology, and Esthetics
- Board of Medicine

Legal Landscape (ME)

- OPOR (69 disparate boards!)
 - Accountants
 - Acupunturists
 - Architects
 - Electricians
 - Land Surveyors
 - Plumbers
 - MDs *and* Dos
 - Etc.
- *How can they have adequate expertise for all those boards?!*

The Process: how it starts

- Regulatory inspections (hair salon/barber shop)
- Complaints filed on line
- Civil suits filed in Superior Court

In NH, a new, troubling pre-litigation tactic

- The State's resources to do the work
- Investigation stigma – and pressure
- Distraction and risk
- This may be cautionary tale for other states. *Have others experienced similar issues or trends in your State?*

How to respond

- Subpoenas can be very short fuse requests, and intimidating.
- Staff should alert management if contacted
- Counsel should be present for interviews
- Cooperation with the Prosecuting Attorney can be very helpful in resolving
- Heading off a Board action, especially publicly-reported discipline (including a Settlement Agreement)

Examples

- A complaint
- An *ex parte* board action (e.g. emergency suspension of license)
- Request for a response
- Outcomes: “no further action” vs. proposed Settlement Agreement

Model for success?

- BEFORE the regulators get far along in their investigation, get involved: cooperate where you can; bring legal counsel to interviews
- Try to shape the trajectory of the investigation to satisfy the Board's concerns (that the regulators are investigating)
- If you must, defend at a hearing: talk to the Board
 - OPLC over-reach? Usual suspects? Rush to judgment?



How Can Sulloway Help?

- Attend/defend interviews
- Quash subpoenas/negotiate schedule
- Representation in Board action
 - Negotiation
 - Defense at a Hearing

Handling Press Inquiries/Preparing for “Crisis Communications”

Bradley D. Holt, Esquire
(mostly healthcare litigation)

Kevin O’Shea, Esquire
(Chair, Privacy Data Protection, and Cyber Liability Practice)

Strategic considerations

- Old school: “no comment”
- Trending (in the northeast): plaintiffs’ bar is getting more aggressive about using media attention as a tactic.
 - *The Maine attorney with the PR firm in court*
 - *The NH attorney who calls the reporters (and leaks)*
 - *Reporters are looking for stories: whose side do they tell?*
- Should defendants change their usual approach? How? (And how not?)

Ethical Issues - HIPAA

- HIPAA – if the issue involves a resident's health/healthcare, you will be limited in what you can say
- (If the resident or their family are bringing claims, they will not have the same constraints.)

Rules of Professional Conduct

(a) A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

(b) A statement referred to in paragraph (a) will more likely than not have such an effect when it refers to a civil matter triable to a jury

“Safe harbor” for statements

A lawyer may state:

- (1) the claim, offense or defense involved and, except when prohibited by law, the identity of the persons involved;
- (2) information contained in a public record;
- (3) that an investigation is in progress;
- (4) the scheduling or result of any step in litigation;
- (5) a request for assistance in obtaining evidence and information;
- (6) a warning of danger concerning the behavior of a person involved
(when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest...)



(Maine) RULE 3.6 TRIAL PUBLICITY

A lawyer ... representing a party to a civil cause shall not make or participate in making any extra-judicial statement which poses a substantial danger of interference with the administration of justice.

Practical issues

- Residential facility crisis management is a specialized area that few public relations firms have experience handling.
- Setting up help in crisis is probably too late.

Objective

- To create an effective communications strategy that can be implemented as part of your organization's emergency management plan, so you are prepared to move forward if something unpredictable occurs.

Plan

- “Plans are nothing; planning is everything!”

Dwight D. Eisenhower

“... the very definition of ‘emergency’ is that it is unexpected, therefore it is not going to happen the way you are planning

...if you haven't been planning you can't start to work, intelligently at least.

That is the reason it is so important to plan, to keep yourselves steeped in the character of the problem that you may one day be called upon to solve--or to help to solve.”

Develop a playbook, vet it (and practice it), to avoid missteps, delays, and confusion.

- Put a crisis communications plan in place before you need one, so the team knows what to do if something unexpected happens.
- A crisis plan includes company protocols, addresses information flow, names a company spokesperson and outlines how and if you will communicate with the media.

Crises could range from:

- weather events,
- illness outbreaks,
- high profile accidents or injuries,
- elopements,
- allegations of abuse or neglect.

Practice for an incident

- Prepare a process, assign roles
- Develop checklists for aspects of the response and resources you might need
- Have an “exercise control team” run a table top exercise
 - FUN! (role players make it realistic)
 - Team building
 - Develop some muscle memory for the real thing.



Develop a Response Book

- Have the numbers and names of first calls
- Have team members' contact information and roles
- checklists

Line up Resources

- There are industry checklists to borrow
 - Cyber hacking event
 - Active shooter event
 - Insurance policy reporting requirements

CISA website



OVERVIEW

An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization *before, during, and after* a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a cybersecurity [list](#) of key people who may be needed during a crisis.

BEFORE A CYBERSECURITY INCIDENT

- **Train the staff.** All staff need to understand their role in maintaining and improving the security of the organization. That includes knowing how to report suspicious events. Be gracious when people report false alarms. Reward people who come forward to report suspicious events as part of your commitment to a culture of security.
- **Review your plan with an attorney.** Your attorney may instruct you to use a completely different IRP template. Attorneys often have preferences on how to engage with outside incident response vendors, law enforcement, and other stakeholders.
- **Meet your CISA regional team.** You can find your [regional office information here](#). Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cybersecurity Advisors (CSAs), Emergency Communications Division Coordinators, and other CISA personnel to handle a wide array of needs.
- **Meet your local law enforcement agency (LEA) team.** In coordination with your attorney, get to know your local police or FBI representatives. The time to figure out how to notify LEA representatives isn't in the heat of battle.
- **Print these documents** and the associated contact list and give a copy to everyone you expect to play a role in an incident. During an incident, your internal email, chat, and document storage services may be down or inaccessible.
- **Develop an incident staffing and stakeholder plan.** What roles will everyone play? Which people and groups will need to be notified that won't be top of mind during the incident? Examples include the board of directors, key investors, and critical partners.
- **Review this plan quarterly.** The best IRPs are living documents that evolve with business changes.
- **Prepare press responses in advance.** If a reporter calls you, claiming to have data stolen from your file servers, what will you say? Having a good "holding statement" will help.
- **Select an outside technical resource/firm** that will investigate potential compromises.
- **Conduct an attack simulation exercise**, sometimes called a tabletop exercise, or TTX. A TTX is a role-playing game where a facilitator presents a scenario to the team. The exercise might start with the head of communications receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game to see how everyone plays their role. Every sports team rehearses, and you should too!

DURING A CYBERSECURITY INCIDENT

- **Assign an Incident Manager (IM).** This person leads the response. They manage communication flows, update stakeholders, and delegate tasks. However, the IM does not perform any technical duties. During a time of crisis, time dilation affects people's perception of time passing. The IM will monitor the clock to avoid that common problem. The IM may also lead the retrospective meeting (outlined below) to gather lessons learned.
- **Assign Tech Manager (TM).** The TM will serve as the subject matter expert. They will bring in other internal and possibly external technical experts (with the consent of the IM and possibly your attorney!)
- **Assign Communications Manager (CM).** The CM will interact with reporters, post updates on social media, and may interact with external stakeholders (like shareholders).

AFTER A CYBERSECURITY INCIDENT

- **Hold a formal retrospective meeting** (sometimes called a "postmortem"). In the retrospective, the IM will report out the known incident timeline and ask for additions and edits. They will then ask for analysis from the incident response team and suggest areas for improvement.
 - **Note: Retrospectives must be blameless.** For retrospectives to have any value, all participants need to feel free to openly discuss the incident in a safe and supportive environment. Security incidents are rarely the result of one person's action. They are almost always the result of a failure of the overall system. The retrospective will examine *people, processes, and technologies*. The focus should be on the *processes* and ways to improve them.
- **Update policies and procedures** based on the retrospective meeting.
- **Communicate** the findings to your staff. Transparency builds trust and many staff will appreciate hearing how seriously the executives consider security. That's how you build a culture of security.

SEE ALSO

- NIST guidance: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- CISA guidance: <https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability>

Incident Handling Checklist

The below checklist provides guidelines to handlers on the major steps that should be performed in case of cybersecurity incidents. It does not dictate the exact sequence of steps that should always be followed. The actual steps performed may vary based on the type of incident and the nature of individual incidents.

Detection and Analysis	
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
Post-Incident Activity	
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)

e.g. ConnectTeam's version...

Incident Report Checklist

Date: [Date of incident]

Incident ID: [Assigned Incident Identification Number]

1. Incident Details:

- **Date:**
- **Time:**
- **Location** (Specific area within the construction site):
- **Project Name:**
- **Phase of the Project** (if applicable):

2. Incident Reporting Information:

- **Name of Person Reporting:**
- **Designation:**
- **Contact Number:**
- **Email:**
- **Name of Supervisor/Foreman** (if applicable):

3. Incident Type:

- Fall from Height
- Struck-by/Struck-against
- Caught-in/Between
- Electrical Incident
- Slip, Trip, and Fall
- Equipment Malfunction
- Fire/Explosion
- Hazardous Material Exposure
- Near Miss/Close Call
- Other (Specify):

4. Incident Description:

[Provide a detailed narrative of what happened before, during, and after the incident. Include the sequence of events, weather conditions, and any contributing factors. Use additional sheets if needed.]

Press Inquiries

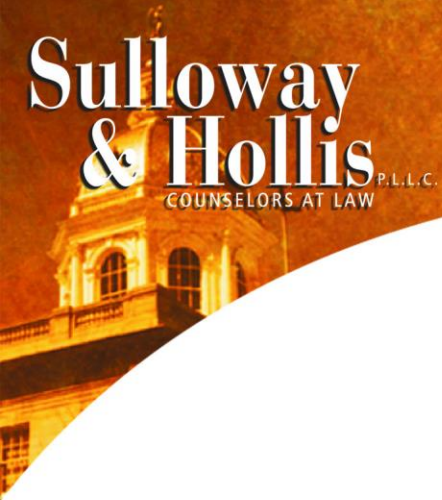
- Getting your message out in a timely manner is important because crises can cause long term reputational damage
- Negative publicity can cause lingering effects that damage a business financially as well as how it is perceived by the community

Lay the groundwork in advance

- Cultivate pre-vetted, pre-approved relationships in advance with a PR firm, Cyber expert, legal counsel, restoration specialists.
- “Reputation repair services” can monitor your online profile and address any damaging information.

Practice for press inquiries

- Assign a designated spokesperson
- help your managers establish protocols for reporting and updating
- designate duties
- ... then practice the plans in mock emergency drills.



The New Hampshire Privacy Act

RSA 507-G

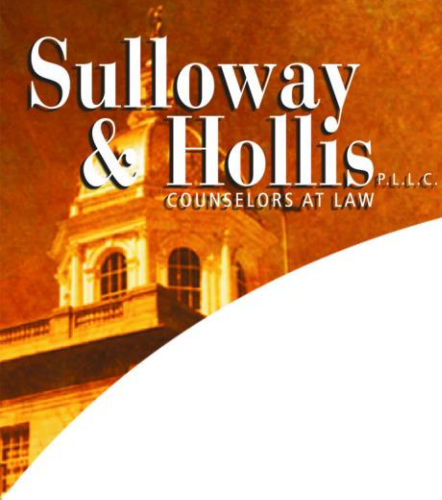
Kevin M. O'Shea, Esquire
Chair, Privacy Data Protection, and Cyber Liability Practice

The Legal Landscape

- On March 7, 2024, Governor Chris Sununu:
 - Signed SB255-FN
 - An Act relative to the expectation of privacy into law
 - Codified as RSA 507-H
 - Effective Date: January 1, 2025

The Legal Landscape

- There is no comprehensive federal privacy statute.
- There are sectoral federal privacy statutes
 - Gramm-Leach-Bliley Act (GLBA)
 - “governs the treatment of nonpublic personal information about consumers by financial institutions.”
 - Health Insurance Portability and Accountability Act (HIPAA)



The Legal Landscape

- Some states have made efforts to create state privacy statutes similar to California's Consumer Privacy Act ("CCPA").
 - New Hampshire's statute in part mirrors the basis of Connecticut's statute; interesting, NH is significantly smaller than other states with existing statutes.
 - Maine is currently considering its own Data Privacy and Protection Act, which has been described as the "the strongest data privacy law in the nation" if passed.

Thresholds

- This chapter applies to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state that
 - (a) controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
 - (b) controlled or processed the personal data of not less than 25,000 consumers and derived more than 25 percent of their gross revenue from the sale of personal data.

Consumers & Personal Data

- "Consumer" means an individual who is a resident of New Hampshire.
- "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.
 - Examples: personal identifiable information (PII)
 - Names, phone numbers, addresses, DOB, SSN, email address, location, identification card numbers, IP address, physical descriptors
 - NB: the statute does not define what exact information is "linked or reasonably linkable to an identified or identifiable individual."
 - Arguably, that is vague language and likely could lead to violations because of ambiguity.

Controllers & Processors

- Controller:
 - Legal entity (incorporated partnerships/associations or public authority) or individual (sole trader, partner in an un-incorporated partnership) e.g. Could be a hospital or a health care facility, if an entity controls the purpose and means of processing of the data
- Processor:
 - It acts on behalf of the controller and serve the controller's interests (company; consultant) e.g. mail house, marketer, on-line targeted mailings

Controllers & Processors

– Example

- A company wants to host a special deal for members and uses a third party to send out advertising to their membership, the third party is acting on behalf of the company to send the deal to membership by email, mail, etc.
- If a health care facility asked a third-party advertising company to mail marketing materials to folks on a list they created,
- The health care facility is the controller and the advertising agency is the processor.

– Controllers make the decisions and processors do the actions

Who is Exempt?

- Body, authority, board, bureau, commission, district or agency of New Hampshire or any political subdivision of New Hampshire
- New Hampshire non-profit organizations
- New Hampshire Institution of Higher Education
- National Securities Association that is registered under 15 U.S.C. section 78o-3 of the Securities Exchange Act of 1934, as amended
- Financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq.; or
- A covered entity or business associate, as defined in 45 C.F.R. 160.103(b)

What is Exempt?

- Protected health information under HIPAA, unless de-identified
- Patient-identifying information
- Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice or personal data used or shared in
- Information and documents created for purposes of the Health Care Quality Improvement Act of 1986
- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act

What (else) is Exempt?

- The collection, maintenance, disclosure, sale, communication or use of any personal information under the Fair Credit Reporting Act.
- Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act

More that is Exempt...

- Collecting, using, distributing, etc. personal data outside the scope of HIPAA:
 - Patient emails/phone numbers
 - Patient addresses
 - Collecting data on which patients have government benefits/VA benefits
 - Any data is used for targeted ads

Must Do in Advance (RSA 507-H:4, II):

Create a "secure and reliable means" for the consumer to exercise rights under section.



Describe the "secure and reliable means" to make requests in your privacy notice.



Create an opportunity for the consumer to designate an authorized agent in accordance with RSA 507-H:5 to opt out of processing their personal data for purposes of RSA 507-H:4, III(e) on behalf of the consumer.

Exception: If the processing of personal data is a minor child's data, the parent or legal guardian may exercise on behalf of the child.

Exception: If the processing of personal data concerns a consumer who is subject to guardianship, conservatorship, or other protective arrangement, the guardian or conservator of the consumer may exercise on behalf of the consumer.



Establish the appeal process. (507-H:5 (IV)) Details the process and 60 day timeline.



Determine amount you would charge consumers for unfounded requests and put it in your policy.

Must Do to Comply (RSA 507-H:4, III):

Respond to consumer requests without undue delay, but not later than 45 days after the request.

What if I need an Extension? Cite: (III)(a)

Consider complexity of and the number of the consumer's requests.



Determine that an extension is reasonable.



Inform the consumer of the extension **and** the reason for the extension **within** the initial 45-day response period.



Take an additional 45-day extension.

What if we decline the request? Cite: (III)(b)



Inform the consumer without undue delay, but not later than 45 days after the request, and inform the consumer of the justification for not taking action. Provide the consumer with instructions to appeal the decision.

Can we charge if the request is unfounded?



If requests are “manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover administrative costs of complying with the request or decline to act on the request. The controller has the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

What if the controller cannot authenticate a request to exercise any of the rights afforded under section I(a)-(d) by using commercially reasonable efforts? Cite: (III)(d)



The controller is not required to comply with the request and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right(s) until the consumer provides additional information reasonably necessary to authenticate the consumer and their request.



What about opt-out requests?



Controllers are not required to authenticate opt-out requests.

What if we deny an opt-out request?

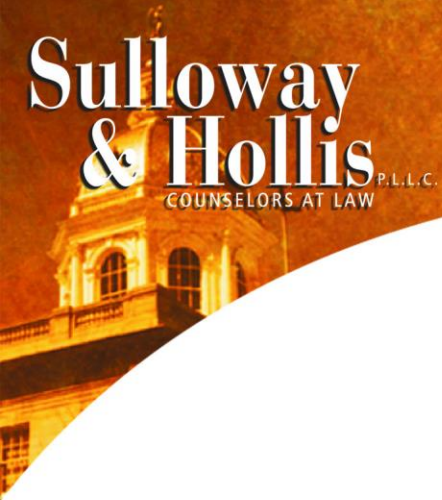
Controllers may deny opt-out requests if the controller has a “good faith, reasonable and documented belief that such request is fraudulent.”



Send notice to the person who made the request and disclose that the controller believes the request is fraudulent, why the controller believes the request is fraudulent, and that the controller shall not comply with the request.

How Can Sulloway Help?

- Privacy Audit for State and Fed Programs
- Drafting/Compliance of Privacy Policies
- Drafting/Compliance of Forms
- Handle/Advise Requests from Consumers
- Handle/Advise Inquiries from Regulators
- Partner with Technical Vendors



Private Equity Funding Litigation

Christopher Pyles, Esquire

Co-Chair, Labor & Employment practice group

Is TPLF a four letter word?

- What is it?
- Why should I care?
- How should I respond?



TPLF – Third Party Litigation Funding Is ...

- A process where third parties underwrite legal claims in exchange for a cut of the proceeds;
- A growing investment market for hedge funds and private equity firms; and
- A burgeoning multi-billion dollar industry.



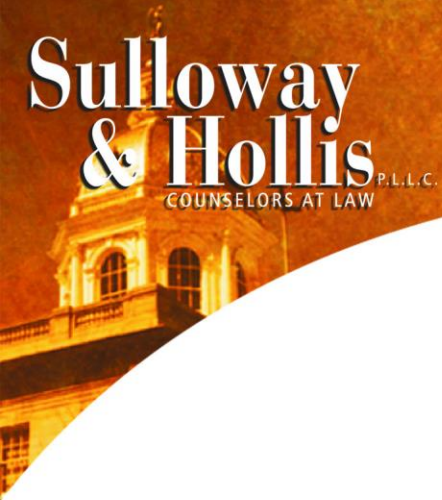
Employers should be concerned
because litigation funded by outside
investors will probably ...

- Incentive more lawsuits;
- Increase costs of discovery; and,
- Impact mediation and verdict values.



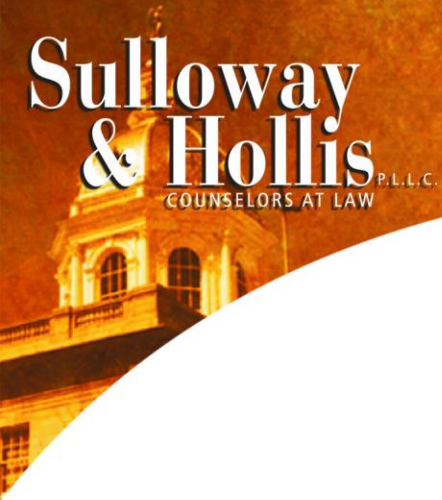
What is the legal landscape for TPLF?

- Maine and New Hampshire;
- Other states; and,
- Federal action.



How can Sulloway Help?

- Educate employers;
- Encourage engagement and lobbying; and,
- Mitigate litigation risks through trainings and advice.



Whistle-Blowers & *Qui-Tam* Relators, in 10 minutes or less!

Robert L. Best, Esquire
Chair, Business Law Practice Group

What (who) is a Whistle-Blower?

- What information does a whistle blower report?
- Who do they report it to?
- What happens next?
- How does a whistle-blower gain advantage by reporting information?

Employee discipline in the whistle-blower context

- Can you fire a whistle-blower?
- What if their performance warrants it?
- What if business conditions warrant it?
- What if you go out of business?




What is a *Qui Tam Relator*?

- Are they employees, patients, members of the public?
- Are they whistle blowers?
- What do they get out of making a report about your organization?

What are the take-home lessons?

- How do you protect your organization from the impact of Whistle-blowers?
- What about protection from *QuiTam* cases?



Sulloway & Hollis P.L.L.C.

COUNSELORS AT LAW

- Questions?

- How Can Sulloway Help?

TRUSTED ADVISORS FOR CHANGING TIMES

BUSINESS & CORPORATE LAW | HEALTH LAW | LABOR & EMPLOYMENT LAW
SCHOOLS & EDUCATIONAL LAW | LITIGATION | DOMESTIC RELATIONS | REAL ESTATE LAW
STATE TAXATION | TAX, TRUSTS & ESTATES | INSURANCE COVERAGE, BAD FAITH AND REINSURANCE