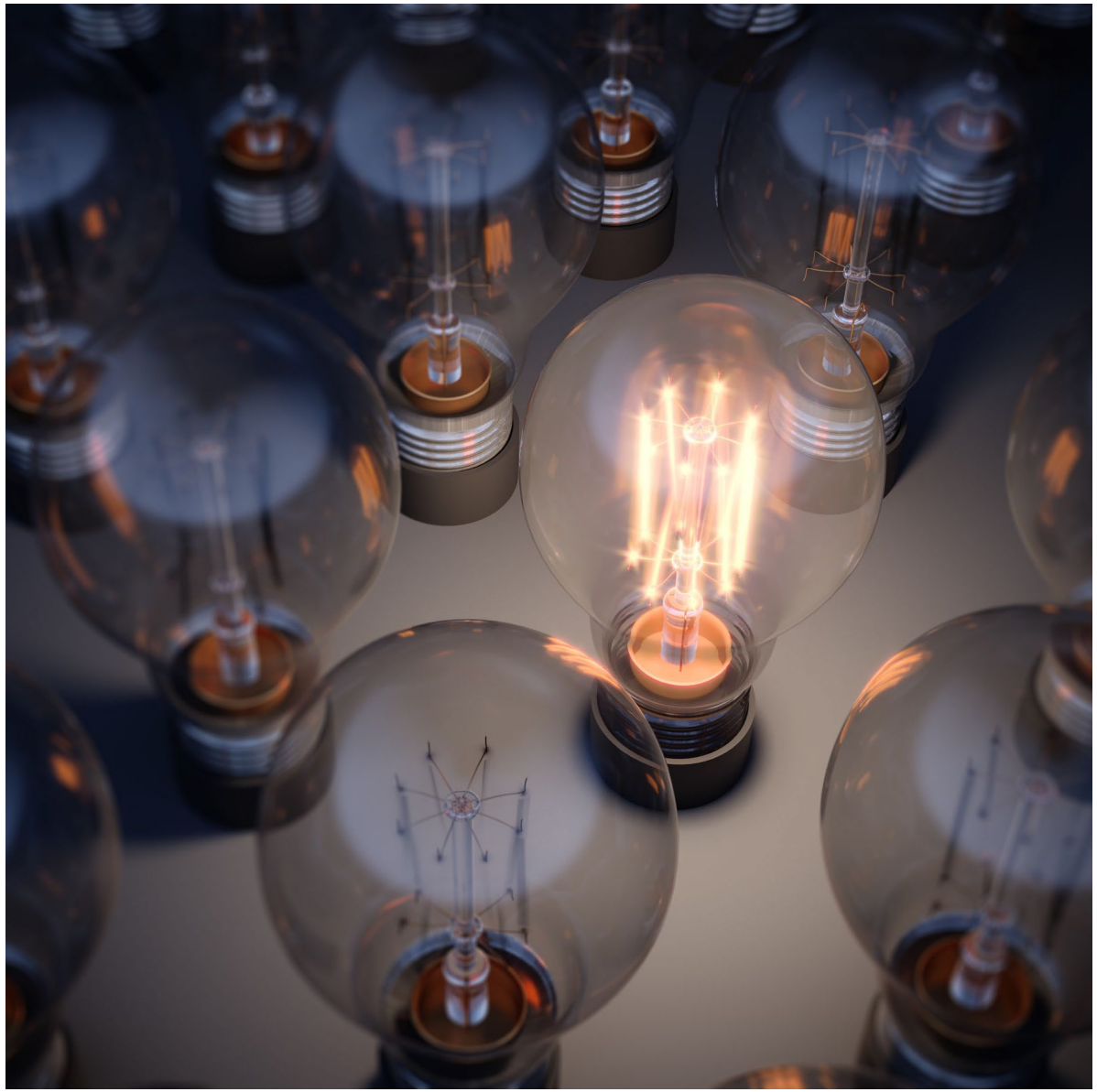
GASB Update for Hospitals: What's on the Horizon for 2025?

January 30, 2025

forvis mazars

Agenda

1. GASB Update – Standards Effective in 2025
2. Provider Panel Dialogue
3. Cybersecurity Hot Topics
4. GASB Update – Recent Standards & Projects
5. Stay warm, earn CPE, and have fun!



© 2025 Forvis Mazars, LLP. All rights reserved.

Meet Today's Presenters

Brian Pavona, Moderator

Partner, Healthcare Assurance
Forvis Mazars

312.270.2506 // brian.pavona@us.forvismazars.com

Danielle Zimmerman, Panelist

Partner, Healthcare Assurance
Forvis Mazars

972.361.3740 // danielle.zimmerman@us.forvismazars.com

Daron Tarlton, Panelist

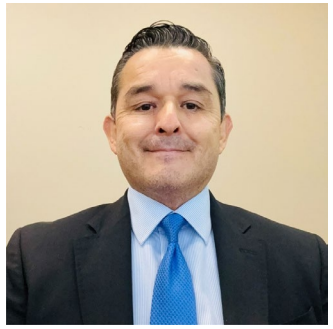
Partner, Healthcare Assurance
Forvis Mazars

813.425.1339 // daron.tarlton@us.forvismazars.com

Ben Owings, Panelist

Director, Healthcare IT Risk & Compliance
Forvis Mazars

864.923.2914 // ben.owings@us.forvismazars.com



James Garcia, Panelist

Controller
University Health
San Antonio, Texas

Terri Contreras, Panelist

Chief Financial Officer
Uvalde Memorial Hospital
Uvalde, Texas

© 2025 Forvis Mazars, LLP. All rights reserved.

GASB Update

Standards Effective in 2025

forvis mazars

GASB 100, Accounting Changes & Error Corrections

Effective for fiscal years beginning after June 15, 2023

Accounting changes

- Change in principle – retrospective with prior-period restatement
- Change in estimate – prospective, recognize in period of change
- Change in reporting entity – retrospective to beg. of period of change

Correction of error – retroactive restatement w/prior period restated

Display cumulative effect adjustment/restatement of beg net position

Tabular disclosure of effects on beg net position for each type

© 2025 Forvis Mazars, LLP. All rights reserved.

forvis mazars

GASB 101, Compensated Absences

- Effective for fiscal years beginning after December 15, 2023
- Recognize liability for leave not used if it accumulates, services have been rendered, & likely to be used or paid/settled
- Recognize liability for leave when it commences if dependent on sporadic event, *e.g.*, military, parental, jury duty (excludes sick leave)
- Recognize liability for leave when taken for unlimited & holiday leave taken on specific date
- Do not recognize liability for leave if likely to be settled through conversion to pension/OPEB

© 2025 Forvis Mazars, LLP. All rights reserved.

GASB Statement 101 Implementation

Provider Panel Discussion

GASB 101, Compensated Absences – Panel Discussion

How have you prepared for implementation?

Any changes in policies/procedures, systems, data capture?

Look at overall benefits being offered?

Significant judgments/estimates?

© 2025 Forvis Mazars, LLP. All rights reserved.

Cybersecurity

Hot Topics & Best Practices

forvis mazars

Cyberattacks in the News

HEALTH TECH

Idaho hospital diverts ambulances, turns to paper charting following cyberattack

By Annie Burky • Jun 1, 2023 04:00pm

Cybersecurity | Emergency Care | Privacy and Security | cyberattack

After ransomware attack, state's second-largest health insurer says patient data stolen

Point32Health says current and former members of Harvard Pilgrim Health Care may have been affected

By Jessica Bartlett Globe Staff, Updated May 23, 2023, 7:38 p.m.

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.

Hacking healthcare: With 385M patient records exposed, cybersecurity experts sound alarm on breach surge

Cybersecurity experts say healthcare companies must harden their defenses, but it may require regulators and lawmakers to raise the bar on security standards.

Cyberattack disrupts health-care system's services in several states

California-based Prospect Medical Holdings had some services shut down down at affiliated locations, and others were forced to rely on paper records

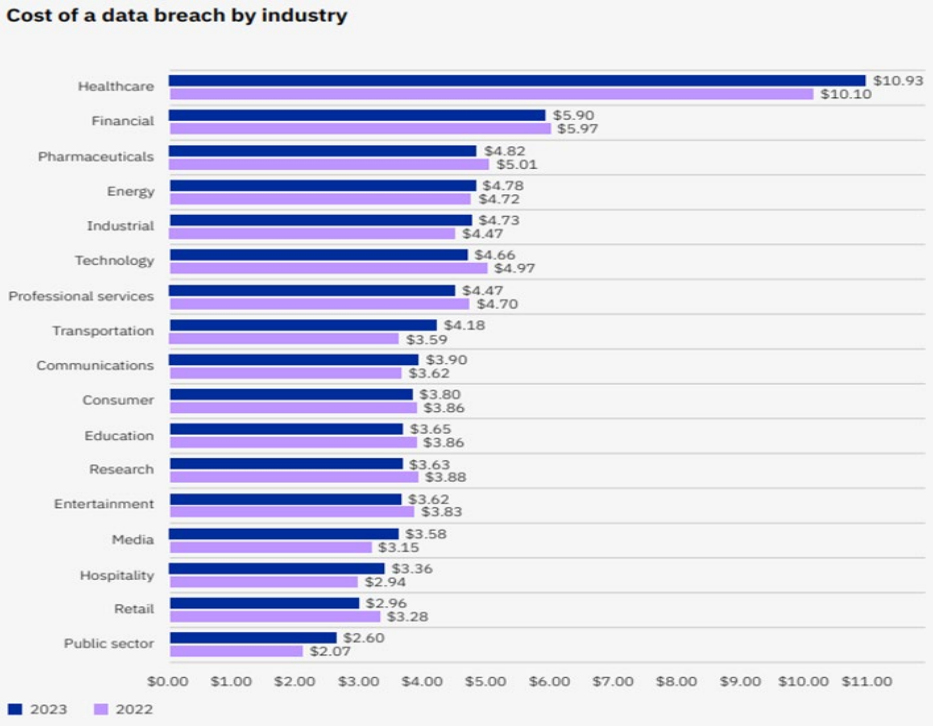
Clockwise from top left: 1 A. Burky, fiercehealthcare.com, June 1, 2023; 2 J. Bartlett, bostonglobe.com, May 23, 2023; 3 K. Collier, nbcnews.com, June 12, 2023; 4 S. Avi-Yonah & K. Rempfer, washingtonpost.com, August 5, 2023; 5 S. Liss & J. Ye Han, healthcaredive.com, March 9, 2023

© 2025 Forvis Mazars, LLP. All rights reserved.

Cost of a Data Breach Including Ransomware

Healthcare was the highest-cost industry for the 14th year in a row.

The average total cost of a breach in healthcare increased from $10.10 million in the 2022 report to $10.93 million in 2023, an increase of $0.83 million or 8.22%. Healthcare is one of the more highly regulated industries & is considered a critical infrastructure by the U.S. government.



$10.93 million

Average cost of a breach in the U.S., the highest of any country[1]

200 days

Average time to identify and contain a data breach[1]

95%

Percentage of organizations that have had more than one breach[2]

Data breaches in high data protection regulatory environments and **critical infrastructure** tended to see costs accrue in later years following the breach. In ***highly regulated industries***, an average of **24% of data breach costs were accrued more than two years** after the breach occurred. Regulatory & legal costs may have contributed to higher costs in the years following a breach.

[1] "Study Finds Average Cost of Data Breaches Continued to Rise in 2023," morganlewis.com, March 6, 2024.
[2] "IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs," newsroom.ibm.com, July 24, 2023.

© 2025 Forvis Mazars, LLP. All rights reserved.

Data Breach Impacts

Reputation Risk

Damage to Brand

Negative Publicity

Damaged Employee Relationships

Operational Disruption

Damaged Third-Party Relationships

Lost Productivity

Diversion of Resources

Regulatory Response

Deceptive or Unfair Trade Charges

Regulatory Scrutiny

Regulatory Sanctions/MOUs

Financial Loss

Regulatory Fines

Legal Liability

© 2025 Forvis Mazars, LLP. All rights reserved.

Be Prepared Through Best Practices

Backup & Recovery

- Maintain offline, encrypted backups of data so it is protected & readily accessible in case of a ransomware attack.
- Test backups & backup procedures on a regular basis.

Source: CISA.gov, Ransomware Guide

Configuration Hardening

- Restrict usage of PowerShell.
- Disable Remote Desktop Protocols.
- Secure domain controllers including patching & updating.
- Configure firewalls to block known malicious IP addresses.
- Restrict user permissions for installing & running software.
- Implement software restriction policies & application whitelisting.
- Network segmentation through virtualization & separation.

Incident Response Plan

- Create, maintain, & exercise a basic cyber incident response plan & associated communications plan.
- Include response & notification procedures for a ransomware incident.

Email Security & Awareness

- Scan all incoming & outgoing emails to detect & filter threats, such as phishing & spooking emails, & executable files.
- Implement training & awareness programs including regular phishing simulation exercises.

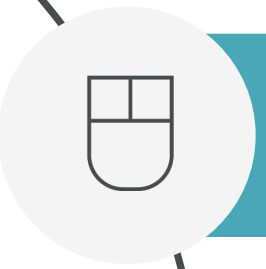
Note: This is not meant to be a comprehensive list of ransomware best practices but rather an overview of key highlights to mitigate the risk of ransomware.

© 2025 Forvis Mazars, LLP. All rights reserved.

Cybersecurity

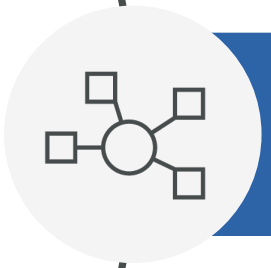
Provider Panel Discussion

Cybersecurity – Provider Panel Discussion

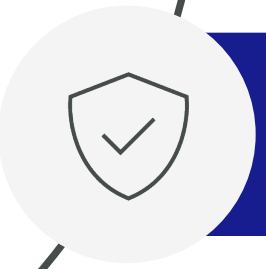


Have you been impacted by any recent cyber events?

- Change Healthcare, etc.



Impacts across organization – finance/accounting, operations, risk, governance



Taken any actions in response?

© 2025 Forvis Mazars, LLP. All rights reserved.

GASB Update

Recently Issued Standards & Projects

GASB 102, Certain Risk Disclosures

Effective for fiscal years beginning after June 15, 2024

Requires entities to:

- Assess whether concentration or constraint makes the entity vulnerable to the risk of substantial impact
- Assess whether an associated event has occurred or likely to occur within 12 months of FS issuance
- Disclose the concentration/constraints, each identified event, and actions taken by management prior to issuance to mitigate the risk

© 2025 Forvis Mazars, LLP. All rights reserved.

GASB 103, Financial Reporting Model Updates

Effective for fiscal years beginning after June 15, 2025

Makes amendments to MD&A requirements

For proprietary funds/business-type activities:

- Defines operating & nonoperating revenues
- Requires separate presentation of noncapital subsidies
- Combines extraordinary items & special items into one “unusual or infrequent items”
- Requires supplementary information of revenues by major source

© 2025 Forvis Mazars, LLP. All rights reserved.

forvis mazars

GASB 104, Disclosure of Certain Capital Assets

Effective for fiscal years beginning after June 15, 2025

Requires capital asset disclosures be broken out separately for the following:

- Lease assets by major class of underlying assets (GASB 87)
- PPP RTU assets by major class of underlying assets (GASB 94)
- Subscription-based IT assets (GASB 96)
- Other intangible assets by major class of assets

Requires disclosures (by major class of asset) for capital assets **held for sale**:

- Separate disclosure of historical cost and accumulated depreciation/amortization
- Carrying amount of debt for which the assets are pledged as collateral

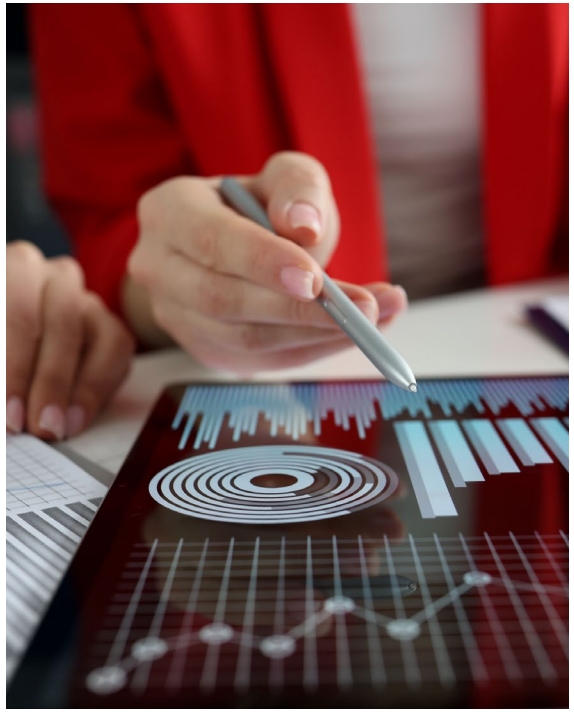
© 2025 Forvis Mazars, LLP. All rights reserved.

GASB Projects

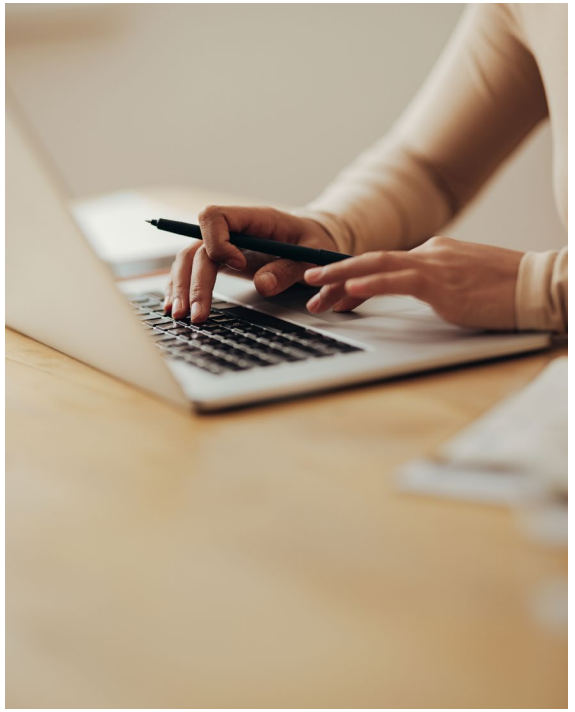
Subsequent Events

Going Concern & Severe Financial Stress

Classification of Nonfinancial Assets



Revenue & Expense Recognition



© 2025 Forvis Mazars, LLP. All rights reserved.

Questions?

Contact

Forvis Mazars

Brian Pavona
Partner
P: 312.270.2506
brian.pavona@us.forvismazars.com

Danielle Zimmerman
Partner
P: 972.361.3740
danielle.zimmerman@us.forvismazars.com

Daron Tarlton
Partner
P: 813.425.1339
daron.tarlton@us.forvismazars.com

Ben Owings
Director
P: 864.923.2914
ben.owings@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2025 Forvis Mazars, LLP. All rights reserved.

Thank You!

forvis mazars