Williams Overman Pierce, LLP
CPAs • Advisors
Summer 2021 Non-Profit Newsletter

The Uniform Guidance – Some Ongoing Pitfalls

By Matthew Cromwell, CPA

We find ourselves years into the implementation of Title 2 Code of Federal Regulations (CFR) 200 – *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). However, a few recurring matters continue to arise that lead to audit findings.

This article will discuss the following areas where we still see findings:

- Subrecipient monitoring
- Equipment
- Period of performance

Subrecipient Monitoring

Three areas where we see challenges on subrecipient monitoring are:

Vendor Versus Subrecipient Analysis

In many instances, this line can be blurred depending on facts and circumstances. Depending on the final determination, different compliance requirements apply to vendors and subrecipients. CFR §200.331 considerations should be clearly documented for each entity engaged. Documentation of this analysis and the final determination should be retained by the organization.

Pre-Award Assessment

CFR 200.332(b), Requirements for pass-through entities, state that an entity evaluate each subrecipient's risk of noncompliance with federal statutes, regulations, and the terms and conditions of the subaward. The pre-award assessment is designed to determine what level of monitoring is required once the subaward is granted as well as determining risk level to the granting organization. Decisions made here determine if the subrecipient is awarded funds in advance or on a cost reimbursement basis, how often program and financial reports are required, or how many site visits or other monitoring actions are required. A granting organization cannot use a blanket pre-award assessment based on the expected amount of grant funding. To be clear, a $20,000 subaward will not receive the same significant level of assessment as a $1 million subaward. For example, grants to subrecipients of

less than $20,000 cannot all be labeled as "low risk" just because of a dollar threshold. Risk assessments need to consider such factors as whether:

- Work is being completed in a high risk location
- First time working as a subgrantee for the organization
- Strong financial controls (and how assessed)

These decisions are all based on the pre-award assessment and certainly it is not a one-size-fits all analysis.

Monitoring

Just as the word implies, the purpose is to monitor subrecipients but entities must also determine if monitoring is uncovering issues (audit findings, lack of financial wherewithal, programmatic departures, etc.). Entities who make subawards need to ensure their monitoring process also ensures subrecipients are addressing and correcting issues identified. Oftentimes, as auditors, we see a file full of single audit reports or financial reports submitted by subrecipients, but nothing has been documented as to the review of these documents. Pass-through entities need to review these items to determine:

1.800.331.5325 wopcpa.com

- What was done by subrecipients—were audit findings corrected?
- Were the financial reports with missing receipts or approvals addressed?

Especially in this COVID environment where in-person monitoring site visits have been rare, the threat of issues is especially high, so take a moment to revisit how you are monitoring from afar and considering reports, calls and other factors that just don't "feel right."

Equipment

Equipment requirements were one of the Uniform Guidance areas where there was little change from prior requirements. However, CFR §200.313, Equipment continues to be a challenge for many organizations. A few points or a "check the box" if you will:

- Property records must be maintained. These should include description, serial number and source of funding for each piece of equipment purchased with federal funds.
- An inventory and reconciliation of each piece of equipment is required, at a minimum, every two years. The Office of Management and Budget (OMB) did not issue any waivers for this requirement even during COVID. Advance approval would have had to be obtained from the federal awarding agency regarding the inability to perform physical inventory counts as required.
- Property is to be kept in suitable working order and maintenance performed. For entities working in remote and/or difficult operating environments, repair/operating costs should be adequately budgeted.
- And finally doing away with a "myth" that some organizations have in regard to equipment compliance testing. We get this question many times a year: If your current year federal expenditures do not include "material" equipment purchases in the current period under audit, the auditor doesn't need to test, right? That is false. If you continue to hold property purchased with federal funds, and it has not yet been disposed, the auditor is still required to test various provisions such as 1) inventory is performed at least biannually; and 2) any disposals, if material, have been disposed in accordance with §200.313 – Equipment e) Disposition.

Period of Performance

An area we have seen regulators focusing on is the use of funds pre-award and costs incurred post award (often referred to as trailing or project closure costs). What is most likely the shortest compliance requirement in the OMB Compliance Supplement (it is literally one paragraph) is often one of the most difficult for organizations to comply with: how to fit all the costs into the actual grant agreement term, more commonly referred to as the "period of performance." It takes significant coordination between all facets of an organization, the program team, the subgrant team and the administrative team to ensure all costs are incurred, including subgrantee costs, and reported correctly. Regulators have continued to raise points of emphasis and findings when identifying costs that occurred after the grant agreement term ends. Yes, they may provide no-cost extensions (see §200.308) for final report submissions. But the regulators have been clear, this does not allow for additional costs to be incurred, contrary to what was for many years seemingly a readily accepted industry practice.

In addition, the recent revisions to the Uniform Guidance have updated the definition of "period of performance" to be "the total estimated time interval between the start of an initial federal award and the planned end date, which may include one or more funded portions, or budget periods." This change is effective for all contracts entered into after Nov. 30, 2020. Entities should stay tuned to see if OMB updates the period of performance audit objectives/procedures in the 2021 OMB Compliance Supplement.

Coronavirus State and Local Fiscal Recovery Funds (CSLFRF)

By Stacey Powell, CPA, and Sam Thompson, CPA

The Coronavirus State and Local Fiscal Recovery Funds (CSLFRF) provide $350 billion in emergency funding for eligible state, local, territorial and tribal governments. The U.S. Department of the Treasury (Treasury) has published an Interim Final Rule that implements and details the provisions of this program. This guidance is applicable to state and local governments. However, it may have an impact on nonprofits, healthcare organizations and institutions of higher education since these funds may be passed through to them from state and local governments.

Key program provisions include:

Use of Funds

Recipients of CSLFRF funds may use funds to:

- **Support public health expenditures,** by, for example, funding COVID-19 mitigation efforts, medical expenses, behavioral healthcare, and certain public health and safety staff.
- **Address negative economic impacts caused by the public health emergency,** including economic harms to workers, households, small businesses, impacted industries and the public sector.
- **Replace lost public sector revenue,** using this funding to provide government services to the extent of the reduction in revenue experienced due to the pandemic.
- **Provide premium pay for essential workers,** offering additional support to those who have and will bear the greatest health risks because of their service in critical infrastructure sectors.
- **Invest in water, sewer, and broadband infrastructure,** making necessary investments to improve access to clean drinking water, support vital wastewater and stormwater infrastructure, and to expand access to broadband internet.

Within these overall categories, recipients have broad flexibility to decide how best to use this funding to meet the needs of their communities.

Funds may not be used to directly or indirectly offset a reduction in net tax revenue due to a change in law from March 3, 2021 through the last day of the fiscal year in which the funds provided have been spent or to make a deposit into a pension fund.

Distribution and Timing of Payments

Treasury expects to distribute these funds directly to each state, territorial, metropolitan city, county and tribal government. Local governments that are classified as non-entitlement units will receive this funding through their applicable state government.

Local governments will receive funds in two tranches, with 50% of the funds provided beginning in May 2021 and the balance delivered approximately 12 months later. However, states that have experienced a net increase in the unemployment rate of more than two percentage points from February 2020 to the latest available data as of the date of certification will receive their full allocation of funds in a single payment. Governments of U.S. territories will receive a single payment. Tribal governments will receive two payments, with the first payment available in May 2021 and the second payment, based on employment data, to be delivered in June 2021.

Additional Guidance and Resources

Additional Treasury guidance and resources including a summary fact sheet, frequently asked questions, a Quick Reference Guide, as well as additional updates as they are released, are available on the CSLFRF page on the Treasury website.

Triaging Data Breaches

By Mark Antalik

A data breach is one of the worst things that can happen to nonprofit organizations, their clients, donors and volunteers. When malicious perpetrators gain unauthorized access to financial information or other personal data, they can steal identities, exfiltrate intellectual property and can cause reputational damages that will affect the organization for years to come.

Information sharing is fundamental to virtually every aspect of business. As an organization grows, information sharing grows along with it—with vendors, contractors, partners and customers. And every one of these relationships present a new set of potential vulnerabilities.

Data breaches are increasing in frequency and can be potentially catastrophic to an organization; therefore, the need for data protection, as well as the way in which it is implemented, must be balanced thoughtfully against strategic and operational needs.

However, given that data breaches are virtually impossible to stop, it is imperative for organizations to build, maintain and follow a sound breach response program. To accomplish this, BDO developed a two-part series with step-by-step methodology to effectively respond to incidents and maintain a program that allows the organization to respond in the wake of crisis.

Series One

1. **Identify, Understand and Communicate –** Processes to identify the potential threat, gain an understanding of the threat and its potential impact, and communicate with the appropriate agencies and other involved or impacted parties.
2. **Respond and Contain –** Responses and efforts to contain or limit data breaches can have significant impacts on an organization's ability to recover from the incident.

Series Two

1. **Perpetuation –** Preservation of evidence will assist in remediating the current breach and may aid in identifying future attempted breaches.
2. **Notification and Identity Monitoring –** Through internal or third-party services, affected parties can be notified of any activity related to their personal information and efforts to remediate and reduce potential impact.

In this article we address the first series. We discuss identifying, understanding and communicating during a

breach situation and how breaches should be managed. In the second series, we will elaborate on perpetuation through digital forensics, as well as outlining approaches to notification and identity monitoring. While it is impossible to eliminate all risk of a data breach, a well-designed program will minimize the negative impact on both short- and long-term business goals.

Identify, Understand and Communicate

There are numerous ways data breaches can occur. An organization's data governance architecture is important for providing the most resilient defenses. When reviewing priorities of a network security program, one must understand that breaches can occur in the following formats:

- Criminal act by outsider (hacking; portable device theft; cloning; burglary)
- Technology failure (firewall or server compromise)
- Insider threat (theft; embezzlement; unauthorized disclosures; collusion; retaliation)
- Human error (lost mobile device; misdirected email or fax [yes…faxes are still in use]; improper configuration of security systems; improper trash disposal; failure to secure physical premises)
- Vendor error (misdirected data, packages or mail)

Given the interconnected nature of our business and personal environments, data breaches can be relatively simple for the persistent malicious perpetrator or discontented insider. Every computer, cellular device, networked system and unsecured Wi-Fi connection represents a potential point of entry.

Unfortunately, most organizations are unaware of how vulnerable they really are; some understand the threat landscape, but they may be focused on other revenue-generating areas of the business. IT professionals, with support from senior leadership, must understand that data breaches are responsible for $400 billion in global losses every year. The problem will only get worse, especially as individuals migrate more of their lives to online systems and resources.

Data breach threats are on the rise for organizations of all sizes and in all industries. Regulators, industry associations and the federal government have begun to act, issuing attestation guidelines and regulatory mandates surrounding organizational cybersecurity programs.

With concern growing among stakeholders, there is building pressure for organizations to prove they have effective controls in place. Organizations must be able to detect and mitigate data breaches that have the potential to disrupt business operations, damage their brand and cause significant financial losses.

Undertaking a comprehensive data protection and cyber risk assessment allows an organization to understand the current state of its program, identify potential gaps and risks and, ultimately, implement and operationalize an effective framework. At a minimum, risk assessments should evaluate:

- **Application Security.** Are your applications protected from outside threats?
- **Data Protection.** Do you know where your sensitive data is stored and how it is protected?
- **Identity and Access Management.** How well do you control who accesses your systems and data?
- **Infrastructure Management.** How well is your network protected?
- **Event Management.** Do you know what to do if there is a cyber breach?
- **Vendor Management.** What are the security practices of third-party vendors who have access to your systems and data?
- **Training.** How aware is the employee population about their cyber responsibilities?

Respond and Contain

Having a plan to respond and contain a breach is a critical step in the breach preparation process. A well-planned response will provide explicit guidance for response resources, reduce emotional conflicts in tense breach situations and demonstrate to clients, donors and volunteers that organizations are in control of the situation and are concerned about protecting personal information.

Consider the following key data breach response-and-contain plan elements:

- **Stay calm.** The steps in dealing with a data breach are mostly common sense. A well-crafted data breach response plan helps avoid reckless decision-making.
- **Assembling a team.** Choose an organization spokesperson in advance such as the general counsel, chief executive officer or another senior leader. Identifying and training backup resources for each role is essential as well.
- **Understanding of the law.** Organizations are sometimes unaware that their public statements, including media appearances and communication with clients, donors and volunteers, may be admissible in court if a lawsuit is filed. Consulting with a privacy attorney and media relations expert can guide language and strategy while also helping to address regulatory and fiduciary responsibilities.
- **Keep the risk within the organization.** Organizations that have been breached can, in turn, unintentionally compromise other organizations by transmitting infected files or malware links. To prevent this, organizations should choose to spend resources and time to fully evaluate the risk and determine measures to reduce it. Measures to reduce risk may include soliciting the expertise of cybersecurity experts that can evaluate and address current and future risk levels for the organization.
- **Deploying a cyber forensic team.** A cyber forensic team will analyze the data breach and determine how the organization was breached, what areas of the enterprise were affected and what information may have been compromised. They can further investigate if the data breach was initiated by an insider, either unknowingly or by nefarious means.

- **Involve legal counsel.** Either internal or external counsel should be engaged for legal guidance and to maintain privilege through the breach response process. Assume that clients, donors, volunteers or other third parties may take legal action against the organization related to the data breach.
- **Notifications.** For data breaches that require notification, a communications plan should include call center guidelines and training. The training might include the tone and message for responding to calls and how any frequently asked questions will be scripted. There will likely be additional notification obligations to regulators or other authorities where counsel and data privacy subject matter experts should be consulted.
- **Communicate on all available channels.** Use the organization's corporate social media channels to frame the story rather than waiting for it to unfold in the media. The media may misinterpret or embellish facts, where the organization can control the narrative. Additionally, organizations should use plain language for these communications rather than potentially confusing technical and legal terminology to express what remediation efforts are being conducted to protect their information.
- **Employee communications.** Communicate with employees so they are aware of the data breach before they hear about it in the media. With knowledge of the breach, employees, with the appropriate approvals, can provide informed communications to their business contacts.
- **Transfer risk to another entity.** This is primarily done through obtaining insurance coverage that specifically addresses the impacts of a data breach. An insurance broker specializing in cyber risk, along with the expertise of forensic accounting and claims consultants experienced in measuring losses, is essential. Keep in mind that communications with insurance agencies do not typically fall under privilege. (See the Spring 2021 Issue of the Nonprofit Standard for an article on cybersecurity insurance.)

Even though customers and individuals are increasingly aware that organizations are at risk for data breach, a breach can be a real test of resiliency. Organizations must plan for a breach and be clear and transparent to clients, donors, volunteers and other third parties about what the organization is doing to protect data. Organizations who meet the crisis head on may even be able to emerge stronger, with a closer connection to their constituencies.

Stay tuned for a discussion of the Series Two topics.

What Higher Education Institutions Need to Know About Tuition Discounting

By David Clark, CIA, CFE, CRMA

Universities and colleges in the U.S. are facing a challenging paradox. Over the past 20 years, tuition rates have increased a staggering amount, significantly outpacing inflation. For instance, the average tuition and fees for private universities ranked by U.S. News and World Report over this time have risen 144%, while the average in-state tuition and fees at public institutions have risen 212%. However, the actual net tuition revenue received by colleges and universities has only moderately increased, with some years even having an average net revenue decrease (inflation adjusted). So, how are colleges charging record-level tuition to students but hardly getting a financial benefit?

The gap between an institution's established cost and the actual cost charged to students is known as the tuition discount. As institutions seek to attract and retain larger, more diverse classes, they continue to offer increased amounts of institutional aid and increase the average tuition discount across programs. This aid may be derived from restricted scholarship funds, but more often is structured as a decision to forgo potential revenue to reduce the cost to the student, which is also known as "unfunded aid."

While tuition rates across the country rise, the average discount rate is reaching unprecedented levels, exceeding 50% for first-year students in recent years. Further, per the National Association of College and University Business Officers' 2019 Tuition Discounting Study, nearly 90% of incoming students are receiving some form of institutional grant. In fact, the percentage of students paying full tuition rates is in the single digits for most higher education institutions. Even the most elite and competitive schools are only achieving approximately one-quarter of students paying full rates.

Public outcry over the volume of student debt and cost of college is at an all-time high, and the current presidential administration is considering various forms of intervention. So, why have colleges and universities not just put an end to the discounting practice and instead lowered tuition? Though the industry has seen a rash of "tuition resets" in recent years (e.g., drastic decreases in tuition rates to reflect the standard average cost paid by students), most institutions are wary of such a strategy and, at times, even advised against it. The reason being, much as with commercial goods, consumers still view a higher price as a sign of an item's superior value (in this case, the education provided).

In actuality, a tuition reset has a relatively minor impact on the amount a student pays to attend a college or university, as students are already only directly responsible for the portion of the cost after institutional aid is applied. Therefore, the cost, which students are currently leveraging public and private grant and loan programs to pay, would still largely equate to the amounts owed under an overall lower tuition rate since most institutional aid is unfunded already. Institutions are using tuition discounting as the primary tool to provide financial support to students and meet or exceed enrollment targets as they consider overall financial aid packaging.

The best-case scenario for colleges and universities is to fund institutional aid through restricted funds and gifts established to provide student scholarships. However, the amount of funding set aside for this purpose in a given budget year likely pales in comparison to the overall tuition discount offered to enrolled students. Therefore, it's critical to understand how operating budgets depend on tuition dollars and ensure that avenues are available to either fund operations through net tuition revenues and other revenue sources, or reduce costs to reflect the reduction in revenue resulting from the tuition discount.

Higher education institutions should also be cognizant of tuition discounting's impact on enrollment. As schools get closer to the start of a new academic year and are looking to fill incoming classes, it may seem enticing to offer greater institutional aid to encourage higher enrollment. While those decisions may make short-term sense (it would be better to bring in 30 cents on the dollar for an additional student than not have any tuition revenue at all), it's important to consider the potential downstream impact of that structure. Will offering more institutional aid now impact the level of discounting needed to recruit and retain future classes? How does aid provided in a student's first year impact the aid offered in subsequent years for that student?

With the higher education sector already facing declining enrollment trends pre-COVID-19 and further uncertainty regarding class sizes in a post-COVID era, an institution's tuition discount can become both a powerful tool and a potential pitfall.

Pulse Check: Is It Time to Update Your Spending Policy?

By Michaela Kay, CPA

2020 was quite the year. While we started off with record highs in the stock market, by mid-March, we saw the fastest 30% decline in the S&P 500 in the history of the index. Since then, we have continued to see many ups and downs, but we still saw overall gains in the stock market.

What does this mean for your organization's spending policy? Is it time for an update?

Most financial experts advise sticking to your plan during tumultuous financial times and embracing volatility, as it can be an organization's best tool to beat inflation and maintain the spending power of invested funds.

However, the events of the past year have shed light on some reasons why an organization should consider updating its spending plan.

Here are a few examples of scenarios that might trigger a policy revision:

1. **The investment fund is underwater.**

   Just as with your personal finances, an organization should not live paycheck to paycheck. If an organization has withdrawn all the income from an investment fund, it may want to consider revising the spending policy to decrease spending. It is healthy to have a cushion of accumulated earnings. That way, when future losses come, it will not be necessary to dip into the corpus in order to keep funding program services.

2. **The spending policy doesn't include a smoothing policy.**

   The most common type of smoothing policy is a simple moving average based on the average balance of the account over a specified period of time (often three years). This helps stabilize spending compared to a policy that focuses on fully spending the annual income or a fixed rate. It also helps to preserve the corpus in the long run.

3. **The organization's goals and needs have changed.**

   Depending on an organization's mission, operations may have changed drastically in the past year. Some organizations, especially in arts and culture, have been shut down. Other organizations, especially those that serve basic needs, may have seen the biggest year in the organization's history. All of these changes have likely led to shifts in financial needs. As a result, it may be necessary to adjust spending in order to use funds responsibly.

4. **The organization received a financial windfall.**

   From time to time, organizations receive bequests or other large contributions. Often these gifts are hard to predict and come at unexpected times. While it is always tempting to spend money, executive management and the board should strongly consider the best use for the funds over the long term. If the contribution is invested, organizations may be able to support programs with very stable funding for years into the future.

Best Practices for Updating Your Organization's Spending Policy

Investment committees should regularly review their organization's investment and spending policies with help from a professional investment advisor. If organizations decide that it is time for a policy update, here are a few next steps:

1. Understand the organization's needs.

When designing a new policy, it is best to start from the ground and work your way up. What are the organization's needs? What is or is not working with the current policy? What is the primary goal for the investment fund? Don't rush into a solution before carefully considering the needs and issues.

2. Seek professional guidance.

Even if the organization has board members or others within the organization with strong financial backgrounds, it may be helpful to seek guidance from a third-party investment advisor. An investment advisor, especially one with a strong background in serving nonprofit organizations, may be able to offer an alternative viewpoint or provide additional ideas about how to meet the organization's objectives. An investment advisor may also be able to model investment and spending policies to give the organization a better idea of how these policies may play out in the future.

3. Start writing.

For any policy to be effective, it must be clear, consistent, specific and realistic. This will likely require several drafts and reviews from multiple people. When drafting, organizations should make sure to compare the new policy with other existing policies for consistency.

4. Seek approval from the board of directors.

Important policies, such as spending policies, should be approved by the board of directors prior to implementation. It's important for organizations to document policy approval in the board of directors meeting minutes and save the policy in a place where it can easily be accessed.

That said, there is no one-size-fits-all spending policy or process to update policies. Each nonprofit is unique and has unique needs for its spending policy. Thus, organizations should consider their options carefully, seek advice and input from others and, if an update is needed, begin writing a new policy with their specific needs in mind.

5 Steps to Maintain Donor Engagement in a Tumultuous Time

By Robby Vanrijkel

COVID-19, the economy and political shifts have resulted in tumultuous times for many nonprofits. Organizational resilience depends heavily on securing funding, and organizations are seeking out new ways to engage with donors to ensure they have the resources needed to continue their missions. Successful nonprofits understand that maintaining these relationships is imperative for the survival and continued growth of their organizations.

To maintain donor engagement during these times, we recommend following these five best practices:

1. **Scenario plan.** While organizations often are aware of their current financial status and most pressing risks, the events of the past year have proven that they need to go beyond assessing the status quo. Some risks are external in nature and incredibly difficult to foresee. Being aware of the full landscape of potential risks and conducting different scenario analyses to determine their impact to the organization are essential to both managing risk and communicating with donors. The future can be hard to predict, so having several scenarios to discuss both internally and externally is imperative to navigating tumultuous times effectively.
2. **Be agile and able to pivot.** During this time, many organizations are responding creatively to the challenges they face, particularly in program implementation and operations. Keeping donors aware of how the organization has pivoted to preserve programmatic impact while ensuring operational excellence is an opportunity to increase donor trust and confidence. Accordingly, this crisis created an opportunity for optimizing operating models not only to address the near-term issues but to secure long-term success by furthering donor relationships.
3. **Understand donor changes.** Many donors are offering flexibility with their grant-making and grant management process in several ways, including repurposing cost savings, extending grant terms, streamlining reporting processes and moving up payments, and converting project grants to general operating support. Ensure you are aware of any flexibility donors may be allowing and assess how these changes could affect your organization. If needed, ask donors to make adjustments that will assist your organization and allow you to increase your impact.
4. **Maintain consistent communication with donors.** Inform donors of the current financial and operational status of your organization and proactively make them aware of constraints when they arise. Donors may have additional funds, programs or tools, such as COVID-related funds, core program funds, system enhancement grants, business planning grants or technical assistance support, to support organizations that are facing challenges. However, donors cannot help you solve problems unless they are aware of them. While this is historically not a common practice, these are unique times that require adaptability from all parties. Work with donors on near-term support options, while seizing the opportunity to advocate for longer-term flexible support.
5. **Be honest.** It's important to share honest updates with donors about what is going well and what isn't to build trust in the midst of this crisis. Understanding and communicating the organization's financial story and potential strategies for the future in an open and transparent manner will help foster stronger relationships. While there is certainly a power dynamic that exists between donors and organizations, nonprofits should not shy away from having these conversations in an honest but delicate way. Many donors prefer to engage in strategically oriented partnerships and focus less on transactional grant-by-grant relationships. Having open and honest conversations will ensure that donors are aware of the organization's needs and how they can help.

While a year has passed since the outbreak of the pandemic, many organizations are still experiencing the aftereffects of the disruption it caused. Despite these challenges, there are measures nonprofits can take to ensure stability with donors. Following these five steps will not only build trust and confidence with donors, but also increase your organization's resilience.

Privacy by Design for Nonprofits

By Gail Spielberger, CIPM

Privacy in the age of modern technology is a major concern for individuals and, moreover, is the focus of laws and regulations directed at organizations that use personal data. The fast-moving digital landscape has not only challenged current lawmakers, but has also resulted in an erosion of public trust in how data is used, stored, transmitted and protected. As organizations, including nonprofits, adopt new technologies, services and business operations, they must be proactive about their data policies and practices to assure individuals their personal data is safe, and likewise reduce the likelihood of data loss, unauthorized disclosure or misuse.

What Is Privacy by Design?

Privacy by Design (PbD) is an approach that considers privacy concepts from the moment a product, service or business process is designed or planned, from inception to implementation. This means that products, services and applications must be designed and developed to protect privacy from the beginning rather than applied later as an afterthought.

Some privacy laws and regulations, such as the General Data Protection Regulation, legally require organizations to apply PbD principles as part of their organizational data practices. As part of these regulations, organizations may be required to provide evidence that they have implemented PbD. This documentation not only demonstrates compliance to regulators, but it also allows your organization to recognize potential privacy issues so risks can be identified and mitigated as projects move forward. Further, these privacy implementations will provide your enterprise with a framework to comply with privacy and data protection laws and regulations, and can strengthen your reputation while differentiating your organization from the competition.

What Does This Mean in Practice?

There are seven PbD principles that serve as an overarching framework for organizations to insert privacy and data protection early, effectively and credibly into information technologies, services or business practices. The information below provides the foundation for your organization to implement PbD principles for new projects where personal data will be collected, used, processed or stored.

PRINCIPLE 1.

Proactive not Reactive; Preventive not Remedial

Anticipate and prevent privacy events before they occur by:

- Creating individual awareness and adoption at the highest levels of the organization, mandating and enforcing high standards as it relates to data protection.
- Promoting a culture of accountability.
- Establishing methodologies and processes to identify data protection risks to ensure they are remediated in a timely and systematic manner.

PRINCIPLE 2.

Privacy as the Default

Build privacy into systems and processes so that personal data is protected automatically, by default, with no additional action required by the individual. This principle can be achieved by:

- Collecting only the minimum amount of data actually needed for specific business purposes and destroying or anonymizing data once it is no longer necessary for those purposes.
- Ensuring personal data is used only for a specific defined purpose and not repurposed unless proper notification and/or consent is provided.
- Not using personal data without a legal basis or consent from the individual .
- Applying reasonable technical and organizational security measures to safeguard against unauthorized access, loss, destruction, modification or disclosure of data.

PRINCIPLE 3.

Privacy Embedded into Design

Integrate privacy into technologies, operations and information architectures to evaluate risks early in the ideation and design processes. Privacy should be embedded in the design and development process, not just considered after the fact. Consider:

- Adopting a systematic approach to embedding privacy in the design and development phases of each project, technology or business process.
- Systematically conducting Privacy Impact Assessments, Data Protection Impact Assessments and Vendor Risk Assessments to clearly identify and assess privacy risks.
- Measuring the risks and considering alternatives or mitigating actions.

PRINCIPLE 4.

Full Functionality – Positive-Sum, not Zero-Sum

Accommodate all business objectives, not just privacy goals, to achieve practical results and benefits for all parties and business units involved by:

- Embedding privacy in a way that does not impair the intended functionality, technical capability or business need.
- Carefully considering all requirements to achieve the optimal multi-functionality of each product.

PRINCIPLE 5.

End-to-End Security – Lifecycle Protection

Personal data needs to be protected throughout the entire information lifecycle from initial collection through destruction. Aim to collect, process, use, share, maintain and destroy personal data in a secure and timely fashion. Consider:

- Building protections for the secure destruction and disposal of personal data when it is no longer needed.
- Monitoring data transfers and ensuring appropriate safeguards and contractual arrangements are in place prior to doing business with third parties.
- Adopting appropriate access controls, encryption standards, data backups and continuous monitoring to ensure personal data remains accurate, with its integrity and availability intact.

PRINCIPLE 6.

Visibility and Transparency

Establish accountability and trust through transparency by informing individuals what data will be collected, how it will be used, and with whom it will be shared. Transparency is not just displaying what the organization does, but also bridging the gap between expectations and reality. To meet this principle, consider:

- Making privacy notices easily accessible and written in clear and simple terms in order to avoid overwhelming the reader with information.
- Mandating and enforcing privacy-related policies for employees and ensuring that vendors are evaluated to identify and mitigate risk in a timely manner.
- Keeping accurate records of data, how it is being used, with whom it is being shared, where it is stored, how long is it being stored for and how the data will be destroyed when no longer necessary.
- Allowing individuals to access and correct their information.

PRINCIPLE 7.

Keep it User-Centric

Respect individual privacy and provide employees, customers and third parties with an effective privacy experience. This means providing them with clear choices about how and when your organization will communicate with them, as well as ways to opt out of having information shared with others and the right to have their data deleted. Consider the individual by:

- Obtaining consent to collect and use individual data in specific ways and allowing them the ability to modify or withdraw their consent if possible.
- Consciously designing products, systems and applications with the individual and their protection in mind.
- Limiting the amount of data your organization collects to reduce overall risk and liability for the individual and the organization alike.

Conclusion

As stated above, Privacy by Design is about examining how your organization uses personal data and what impact that use will have on individuals. By incorporating the aforementioned principles into your operations, your organization will be able to better: capture and mitigate risks, understand the data it possesses, demonstrate compliance to regulators and maintain respect for individual privacy.

Other Items to Note

FASB Proposes Improvements to Discount Rates for Lessees

On June 16, 2021, the Financial Accounting Standards Board (FASB) released a proposed Accounting Standards Update (ASU) related to the Leases standard (Topic 842). The proposed ASU would improve the discount rate guidance for lessees that are not public business entities which includes nonprofit organizations, private companies and employee benefit plans.

Under the new lease standard, that needs to be adopted for fiscal years beginning after December 15, 2021, these entities can utilize a practical expedient so these entities could establish an accounting policy election to use a risk-free rate as the discount rate for all leases. An example of a risk-free rate is a Treasury rate.

However, feedback from many stakeholders was that this risk-free rate election in the current environment was leading to an increase in the entity's lease liabilities and right-of-use assets recorded in the statement of financial position.

The amendments in the proposed ASU address this concern by permitting these entities to make the application of the practical expedient by class of underlying asset instead of entity-wide. In addition, the amendments state that if there is a rate implicit in the lease that can be determined, that rate should be utilized instead of the risk-free rate or an incremental borrowing rate, regardless of whether it has made the risk-free rate election.

Provider Relief Funds (PRF) Reporting Requirements Update

On June 11, 2021, Health Resources and Services Administration (HRSA) released a Reporting Requirements Policy Update related to provider relief fund reporting requirements. The updated Post-Payment Notice of Reporting Requirements seeks to amend the previous reporting requirements released on January 15, 2021. These reporting requirements apply to PRF General and Targeted Distributions (including the Skilled Nursing Facilities (SNF) and Nursing Home Infection Control Distribution). These reporting requirements do not apply to the Rural Health Clinic COVID-19 Testing Program or claims reimbursements from the HRSA COVID-19 Uninsured Program and the HRSA COVID-19 Coverage Assistance Fund (CAF). Additionally, HHS also updated its Frequently Asked Questions (FAQs) as of June 11, 2021.