UHY LLP
Certified Public Accountants

HEALTH CARE INSIDER

VOLUME 5 :: ISSUE 2

In This Issue:

Is Your Nursing Home Certification at Risk?

Did you know that Section 6401 of The Accountable Care Act mandates that nursing homes and other specifically defined providers of medical services must establish a voluntary compliance program as a condition of enrollment with Medicare?

The existence of a voluntary compliance program does not mean you are without risk.

Your compliance program is a strong statement of your organization's intent to proactively comply with Medicare rules, regulations, and laws, and helps ensure that compliance with defined and documented policies, procedures, and employee education.

Best practice organizations continually review their compliance programs to ensure its implementation throughout the organization and adequate documentation exists to support such a claim.

If you don't have a voluntary compliance program, your organization could be at risk to lose its Medicare certification. Having a strong and fully integrated voluntary compliance program is the company's best defense when questions of Medicare compliance arise.

The next level of service

Tablet and Mobile Device Management in Healthcare

Mobile technology has changed business, and for many, their personal lives as well. Mobile connectivity has grown in recent years and healthcare providers are working to keep up with these changes to support their patients and employees.

Regulatory agencies, compliance officers and IT departments are increasingly concerned about safeguarding mobile devices. Smartphones, tablets, and wearables are constantly transmitting data, and their use in health care, if not appropriately managed, may put protected health information ("PHI") and other sensitive corporate data at increased risk.

Background

Mobile Device Management ("MDM") creates a unique challenge to IT. In addition to exponentially increasing the number of data access points that must be controlled, mobile devices are inherently transitory, creating additional challenges to effective monitoring. Healthcare organizations are incorporating mobile technology into their culture in a variety of ways. The myriad of operating systems and devices being implemented throughout organizations further complicates the effort to control data.

COMMONLY USED ACRONYMS

MDM:
Mobile Device Management

CoIT:
Consumerization of IT

BYOD:
Bring Your Own Device

MAM:
Mobile Application Management

MEM:
Mobile Email Management

MIM:
Mobile Information Management or
Mobile Instant Messaging

COPE:
Corporate Owned, Personally Enabled

EMM:
Enterprise Mobility Management

Increased clinical and physician mobility is improving patient care, transforming workflow, boosting productivity, and reducing medical errors. Physicians and clinicians are empowered with immediate access to patient information and other relevant data. Most of the modern workforce has a smartphone, but many also have tablets or laptops. Where organizations have not promoted their use, employees are embracing these tools on their own, as they have become accustomed to their benefits in their personal lives. This trend has become known as the consumerization of IT ("CoIT").

Many employees do not want to carry multiple devices and want to use the same devices at work as they do at home. Many organizations have realized this and adopted "bring your own device" ("BYOD") policies. However, this convenience to employees brings an increased risk to their organizations. This risk applies to every organization regardless of its size.

Regardless of device ownership, healthcare organizations need to assert ownership of their data. Employees and third-parties may access and process data, but each organization is responsible to identify, secure, protect, and monitor their data and its usage. One tipping point for mobile devices in the business is instant access to cloud-based systems that host data, applications, and the processes everyone utilizes–now employees can access all of these from their mobile devices.

Define Scope

The first step in effective MDM is to identify the mobile devices the organization wants to manage. It is not feasible for an organization to support or control every possible device. This scope must be identified to allow effective management of those devices that meet the minimum-security policies the organization has established. It important to communicate this in the BYOD policy to employees so they can plan accordingly as they consider their purchase.

Implement a Policy

Each organization should implement mobile device policies establishing acceptable use, asserting its ownership of its data on the end user device, and requiring the end users to acknowledge the organization's right to access their device. This policy should clearly communicate to the end user that they have no expectation of privacy, that the device may need to be examined, that personal information may be disclosed, and what will happen if the device is lost or stolen or if the employee leaves the organization.

POLICY CONSIDERATIONS

- Approved Devices
- Compliance
- Location Restrictions
- Security
- Applications
- Data Protection
- Agreement
- Employee Privacy

Mobile information management ("MIM") is a device-agnostic strategy that encrypts sensitive data and allows only approved applications to access it. Mobile device policies should consider the existing internal control structure and how the following can be addressed.

- Approved Devices: Which devices will be supported? Consider multiple devices for each user. It is important to register and monitor each device and not assume that each user only has one.
- Compliance: What regulations govern your organization? Perhaps additional requirements need to be considered. HIPAA requires native encryption on every device with access to PHI.
- Location Restrictions: Will the device be restricted to on-premises use? If not, will the organization subsidize or pay any of the monthly data plan expense?
- Security: What security controls will be required – passcode protection, fingerprinting, anti-malware, encryption, VPN, cloud backup?

- Applications: How should applications be restricted – containers, blacklisting, IP scanning, data sharing, cloud services?
- Data Protection: What resources can employees access – email, documents, messaging, file-sharing?
- Agreements: Does the Acceptable Use Agreement cover personal devices and specifically address corporate data?
- Employee Privacy: Is data collected from employees' devices? How is it used? Is it stored securely?

Manage the Devices

MDM focuses on device activation and enrollment, as well as user access provisioning. The next step is to enforce organization policy on the end user devices. Management must decide the extent of their control over user devices. Enrollment should be simple and erase any existing, pre-compliance connections to organizational data. The first step is the Acceptable Use Agreement and acknowledgement of the mobile device policy.

IT should implement a "Deny All" policy for any new devices until the enrollment process begins to ensure compliance with organizational policies. All mobile devices should be quarantined and prevented from accessing data until IT can implement security measures and any other application restrictions. Mobile application management ("MAM") is the software or application delivery, licensing, configuration, maintenance, and tracking. Email is the most common service users may want to access, but careful attention should be given to which applications can access corporate or client data. Automatic backup, data synchronization, and data-sharing services are common ways to lose control of sensitive data.

Next Steps

Mobile device management is a company-specific deployment. The same approach will not be suitable for every organization. Effective enterprise mobility management ("EMM") can lead to operational efficiencies, significant financial savings, and increased productivity. However, the devices supported, security required, and services provided will need to be modified over time to ensure continued compliance with defined policies. Mobile devices are firmly established in today's businesses and organizations need to proactively identify and secure the growing number of access points to their data.

> "Mobile technology has changed business, and for many, their personal lives as well."

Article written by Michael Witt,
Senior Manager
Internal Audit, Risk & Compliance Services

IRS and DOL Gang Up On Employers: Reimbursing Employees' Out-of-Pocket Health Insurance Costs

On September 13, 2013, the IRS and the DOL each issued identical notices - IRS Notice 2013-54 and DOL Technical Release 2013-03 - which adversely impact employers reimbursing their employees, on a pre-tax basis, for their out-of-pocket costs for their health insurance premiums on policies selected by the employee and/or their non-premium medical expenses. The position being taken by these two agencies will be collectively referred to as the "Agency Ruling". The Agency Ruling has been greeted with consternation by those employers who have chosen not to purchase their own group health policy for their employees, but nevertheless want to assist some or all of their employees in obtaining their own health policy on a tax-favored basis. This article explores in greater detail the position being taken by these agencies in this regard.

Q: TO WHAT REIMBURSEMENT ARRANGEMENTS DOES THE AGENCY RULING APPLY?

A: First of all, the Agency Ruling addressed only certain arrangements instituted by an employer whereby the employer reimburses an employee for either (i) his health insurance premiums being charged to him by the insurance carrier of the policy selected by the employee, or (ii) his non-premium medical expenses, or (iii) both such expenses. These reimbursement arrangements can take the form of either a salary reduction cafeteria plan, a Health Reimbursement Account (HRA), a Flexible Spending Account (FSA), or, what the Agency Ruling refers to as an "Employer Payment Plan (basically, an arrangement that solely reimburses an employee for his health care insurance policy premiums). Second, the Agency Ruling only applies to those reimbursement arrangements for which the employer treats its reimbursements as non-taxable to the employee under Section 106 of the Internal Revenue Code. Third, for those arrangements reimbursing the employee for his premium costs, it does not matter if the policy purchased by the employee is acquired by him within or outside of the various state Marketplace Exchanges created under the Affordable Care Act (ACA). For ease of reference only, the above identified reimbursement arrangements are referred to herein as a "Prohibited Reimbursement Arrangement".

Q: WITH RESPECT TO A "PROHIBITED REIMBURSEMENT ARRANGEMENT", WHAT DOES THE RULING HOLD?

A: Because the IRS considers the maintenance of a Prohibited Reimbursement Arrangement as a failure to comply with certain of the provisions of the ACA, It is empowered to assess a penalty against the employer under Section 4980D of the Internal Revenue Code (IRC). Under IRC Section 4980D, the employer is potentially subject to a penalty of $100 for each day the failure occurs per affected employee. If the IRS believes that the failure is unintentional, the penalty cannot exceed $500,000. If, however, the IRS believes that the failure is intentional, there is no maximum penalty. It should be noted that the penalty of IRC Section 4980D does not apply to small employers (i.e., those employers with no more than 50 employees) which provide health care coverage solely through an insured group health plan. Nevertheless, such exception would arguably not cover a Prohibited Reimbursement Arrangement.

Q: ARE THERE ANY REIMBURSEMENT ARRANGEMENTS WHICH WOULD NORMALLY BE CONSIDERED TO BE A PROHIBITED REIMBURSEMENT ARRANGEMENT, BUT WHICH ARE NEVERTHELESS SPECIFICALLY EXCEPTED FROM BEING TREATED AS SUCH UNDER THE AGENCY RULING?

A: The Agency Ruling states that the following reimbursement arrangements are not considered to be Prohibited Reimbursement Arrangements:

1) Reimbursements for premiums paid for Insurance policies that only provide HIPPA "excepted benefits" (namely, accident, cancer, hospital indemnity, stand-alone vision and/or dental benefits); and
2) Reimbursement arrangements that cover only former employees (e.g., arrangements that reimburse former employees for COBRA premiums for coverage under the employer's own insured group health plan); and
3) Reimbursement arrangements that are "integrated" (as discussed below) with the employer's own group health plan and that plan otherwise conforms to all of the applicable requirements of the ACA (referred to herein as an "ACA Compliant Plan").

Q: WHAT IS THE EFFECTIVE DATE OF THE AGENCY RULING?

A: Although there is some uncertainty on this point, in general, the Agency Ruling appears to be effective for the first plan year of the reimbursement arrangement that begins on or after January 1, 2014.

Q: WHAT IS THE OFFICIAL RATIONALE FOR THE AGENCY RULING?

A: The Agency Ruling takes the position that the Prohibited Reimbursement Arrangements violate the ACA by failing to comply with either Section 2711 of the Public Health Service

Continued on Page 5...

Continued from Page 4...

Act (as amended by the ACA) which prohibits annual and lifetime dollar limits on "essential health benefits" (another term introduced by the ACA) or Section 2713 of the Public Health Service Act (as amended by the ACA) which requires that non-grandfathered plans provide certain preventive services without any cost sharing.

Q: HOW DOES A PROHIBITED REIMBURSEMENT ARRANGEMENT VIOLATE SECTION 2711 OF THE PUBLIC HEALTH SERVICE ACT?

A: The IRS maintains that such Arrangements fail to comply with the annual/lifetime dollar limitation because (i) the Arrangement imposes an annual limit equal to what is being reimbursed by the employer (e.g. the cost to the employee of the individual market insurance coverage purchased by the employee through the Arrangement), and (ii) the Arrangement cannot be "integrated" with the coverage being provided to the employee under the individual health insurance policy purchased under the Arrangement. If the Agency Ruling were to allow such integration, then, if the policy purchased by the employee does not impose an annual limit on benefits, the prohibition of Section 2711 of the Public Health Service Act would be satisfied by integrating such prohibition with the subject reimbursement arrangement. Interestingly, the IRS offers no statutory or even regulatory authority for its position that the individual policy being acquired by the employee cannot be "integrated "with the subject reimbursement arrangement. Indeed, this is one of the most criticized aspects of the Agency Ruling.

Q: HOW DOES A PROHIBITED REIMBURSEMENT ARRANGEMENT VIOLATE SECTION 2713 OF THE PUBLIC HEALTH SERVICE ACT?

A: In the view of the IRS, the inherent annual dollar limitation in the Arrangement causes the Arrangement to fail to cover, in all instances, the preventive care Section 2713 is interpreted to require.

Q: SINCE THE "INTEGRATION" OF A REIMBURSEMENT ARRANGEMENT WITH THE EMPLOYER'S OWN GROUP HEALTH PLAN WHICH IS AN ACA COMPLIANT PLAN CAN PREVENT THE ARRANGEMENT FROM BEING CONSIDERED A PROHIBITED REIMBURSEMENT ARRANGEMENT, WHAT ARE THE REQUIREMENTS FOR SUCH "INTEGRATION"?

A: In order for a reimbursement arrangement offered to an employee to be "integrated" with the employer's ACA Compliant Plan, all of the following requirements must be met:

1) The employer must offer to the employee coverage under the employer's ACA Compliant Plan; and
2) Participation in the reimbursement arrangement is limited to those employees and their dependents who also participate in an ACA Compliant Plan (which does not have to be sponsored by the employee's employer - for example, a plan sponsored by the employer of the employee's spouse would suffice for this purpose), and
3) If the reimbursement arrangement reimburses the employee for anything other than the following expenses, then the ACA Compliant Plan must provide "minimum value" (as that term is specially defined in the ACA):

- Co-payments under an employer's group health plan;
- Co-insurance under an employer's group health plan;
- Deductibles under an employer's group health plan;
- Insurance premiums under an employer's group health plan; and
- Health benefits that are not "essential health benefits" (as that term is defined in the ACA).

Q: DOES THE AGENCY RULING ADDRESS THE FEDERAL INCOME TAX CONSEQUENCES TO THE EMPLOYEE IF HIS EMPLOYER NEVERTHELESS CONTINUES TO REIMBURSE THE EMPLOYEE UNDER A PROHIBITED REIMBURSEMENT ARRANGEMENT (AS DEFINED ABOVE)?

A: No. The Agency Ruling does not address the income tax exclusion rule under IRC Section 106 associated with these types of reimbursement arrangements. In other words, the holding in Rev. Rul. 61-146 is not affected. In that Ruling, the IRS was presented with a premium reimbursement arrangement under which an employer reimbursed an employee for his cost of paying the policy premiums of an individual market policy obtained by him. In that Ruling, the IRS ruled that as long as the employee adequately substantiates his premium payments, the amount of the employer reimbursement is excludable from the gross income of the employee under IRC Section 106.

Article written by Richard Dyo, Tax Principal and Don Hughes, Tax Manager

PROVIDING VALUE TO THE HEALTH CARE INDUSTRY

Today's growing and advanced health care industry is a fast-paced environment where regulatory issues, competition, and rapidly changing consumer expectations converge. Managing risks and realizing opportunities becomes a more important focus as health care organizations decide how they will adapt and evolve their business models for long-term survival.

Ensuring today's actions will lead to achieving long-term goals can be a major challenge for anyone. Many health care organizations are unable to address the issues at hand and consider the "big picture" because they are overwhelmed with urgent matters and patient care. UHY LLP's National Health Care Practice brings an understanding of the industry together with innovative solutions that have a positive impact on bottom line. We understand the challenges facing health care providers and facilities.

OUR LOCATIONS

CT New Haven 203 401 2101
GA Atlanta 678 602 4470
MD Columbia 410 423 4800
MI Farmington Hills 248 355 1040
MI Sterling Heights 586 254 1040
MO St. Louis 314 615 1301
NJ Oakland 201 644 2767
NY Albany 518 449 3171
NY New York 212 381 4800
NY Rye Brook 914 697 4966
TX Dallas 214 243 2900
TX Houston 713 561 6500

ADDITIONAL UHY ADVISORS LOCATIONS

IL Chicago 312 578 9600
DC Washington 202 609 6100