NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

SUBCOMMITTEE ON PRIVACY, CONFIDENTIALITY & SECURITY

SECTION 1179 OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

PRESENTATION BY THOMAS WILDER
ON BEHALF OF AMERICA'S HEALTH INSURANCE PLANS
May 6, 2015

Thomas Wilder
Senior Counsel
America's Health Insurance Plans
601 Pennsylvania Ave. NW
South Building, Suite 500
Washington, DC 20004
(202) 778-3255
twilder@ahip.org

Good afternoon Chairman Kloss and members of the Subcommittee. My name is Tom Wilder and I am Senior Counsel at America's Health Insurance Plans (AHIP). AHIP is the national association representing health insurance plans that provide coverage to more than 200 million Americans. Our members offer a broad range of health insurance products in the commercial marketplace and also have demonstrated a strong commitment to participation in public programs. The innovative products offered by our members include high-deductible health plans linked to Archer Medical Savings Accounts (MSAs), Health Savings Accounts (HSAs), and Health Reimbursement Arrangements (HRAs). AHIP also represents a number of financial institutions that provide custodial and/or administrative services to individual consumers and employers in connection with Archer MSAs, HSAs, HRAs, and health Flexible Spending Accounts (FSAs).

I want to thank the Subcommittee on Privacy, Confidentiality & Security for the opportunity to provide comments regarding health care spending accounts and the application of federal and state privacy and data security requirements to these arrangements. In particular, you have asked for feedback regarding how banks and other financial sector businesses are using personal health data in connection with the health care system and the services they provide to HIPAA covered entities. My testimony today will (a) provide an overview of health care spending accounts; (b) describe the respective roles of health insurers, employers, and financial institutions in establishing and maintaining these accounts; and (c) explain the comprehensive framework of privacy and data security standards protecting the collection, use, and exchange of personal financial and health information in connection with health care spending accounts.

Health Care Spending Accounts

Federal law recognizes four distinct types of health care spending accounts that may be used by individual consumers to pay for qualified health care expenses on a tax favored basis – Archer Medical Savings Accounts, Health Savings Accounts, Health Reimbursement Arrangements, and health Flexible Spending Accounts. These accounts allow consumers to be directly engaged with their health outcomes and to make decisions on how best to spend their money on the cost of care.

In each of these arrangements the consumer and/or his or her employer deposits funds into the account that are used to reimburse qualified health care expenses (i.e., medical costs recognized

under Section 125 of the federal tax code) incurred by the individual and family members. Banks and other financial institutions serve as custodians of the accounts and offer administrative and other services, such as debit cards that are linked to the account and used at the health care provider's office, hospital or pharmacy to pay for medical care or prescription drugs. In the case of Archer MSAs, HRAs, and HSAs, the account is typically coordinated with health coverage offered through a health insurer or self-funded group health plan.

Archer Medical Savings Accounts

Archer MSAs were authorized in 1996 as a pilot program in the Health Insurance Portability and Accountability Act (HIPAA). Small employers (i.e., businesses with 50 or fewer employees) set up tax-exempt trust or custodial accounts at a bank or other financial institution for their employees to pay for qualified medical expenses of the employee, spouse or dependents. The employee must be enrolled in a qualified high deductible health plan (HDHP) offered by the employer – for 2015, the deductible for self-only coverage must be between $2,200 and $3,300 with an out-of-pocket maximum limit of not more than $4,450. The deductible for family coverage must be between $4,450 and $6,650 with an out-of-pocket spending maximum limit of not more than $8,150. The HDHP must provide "first-dollar coverage" for preventive care services without any cost-sharing by the consumer. Funds in the account belong to the individual, are rolled-over each year, and may be taken by the individual after they are no longer employed by the business that established the account.

The pilot program for Archer MSAs ended in 2007. Effective January 1, 2008, new accounts may not be established although employers may continue to offer MSAs set up prior to that date and enroll new employees into their MSA-qualified HDHPs. Most Archer MSAs were converted into health savings accounts described below.

Health Savings Accounts

HSAs were established as part of the 2003 Medicare Modernization Act and the first accounts opened in 2004. Since that time, the HSA market has grown considerably – according to AHIP's latest Census of the HSA Market, approximately 17.4 million Americans were enrolled in HSA compatible HDHPs as of the end of 2013. Like Archer MSAs, consumers and employers may only contribute into the account if the individual is enrolled in a qualified HDHP. However, unlike MSAs, a health savings account may be established by an individual consumer or by an employer on their behalf. As a result, HSA-qualified HDHPs are offered in the individual, small group, and large group insurance markets and by self-funded group health plans. HSA funds are

owned by the account holder and may be used at any time for qualified medical expenses – even after the individual is no longer enrolled in the qualified HDHP.

For 2015, a self-only qualified HDHP must have a minimum deductible of not less than $1,300 and an out-of-pocket spending limit no greater than $6,450. Family HDHPs must have minimum deductibles of not less than $2,600 and out-of-pocket limits not exceeding $12,900. The qualified HDHP must provide coverage for preventive services before the plan deductible is met and without any cost-sharing by the enrollee.

Health Reimbursement Arrangements

HRAs were first recognized in guidance from the Internal Revenue Service in 2002. The arrangements are a bookkeeping account of employer contributions to reimburse employees for qualified medical expenses of the employee and family members. Approximately 4 percent of U.S. firms that offer health coverage provide an HRA to employees based on the 2014 Employer Health Benefits Survey from the Kaiser Family Foundation and Health Research & Education Trust.

The HRA is offered as part of a group health plan and funded entirely by the employer who makes a fixed contribution amount each plan year. The plan sponsor decides whether the account funds roll over each year and the employee does not take the funds with them when they leave employment with the employer.

In general, the HRA must be integrated with other group health plan coverage offered by the employer. Individuals enrolled in the HRA must also be enrolled in the employer's plan or another group health plan such as a plan covering the employee's spouse. There are no HRA-related requirements with respect to minimum deductibles or maximum out-of-pocket expense limits for the group health plan coverage.

Health Flexible Spending Accounts

A health FSA is offered by employers through a federal tax code Section 125 "cafeteria plan" as a way for employees to pay for qualified medical expenses on a pre-tax basis. Employees select a specific amount of benefits each year, with a corresponding salary reduction agreement, meaning the employer deducts funds for the health FSA from each paycheck. . Under the tax regulations the annual election amount must be available to the employee at all time, regardless of how much payroll the employer has withheld. If the employee used up the benefits and

terminates employment, the employer may not recoup any part of the costs. In 2015, the annual health FSA contribution limits are $2,550. The employer decides whether unused funds in the FSA roll-over at the end of the plan year – generally, employers may permit employees to carryover up to $500 at the end of the plan year or may give enrollees up to two and a half months after the end of the plan year to use the money for health care expenses.

Establishment and Maintenance of Health Care Spending Accounts

As noted, employers, health insurers, and financial institutions play different roles with respect to the establishment and maintenance of health care spending accounts. As will be discussed in the following section of my testimony, these different roles affect the privacy and data security protections applied to the accounts.

In the case of Archer MSAs and HSAs, the individual consumer is the account holder. They own the funds in the account and may take the money with them when they change jobs or leave employment. The health insurer or employer offering the HDHP coverage will frequently partner with a bank or other financial institution to provide the Archer MSA or HSA, however, the consumer may choose to open the account at a different financial institution. The consumer is responsible for providing enrollment information needed to establish the account (name, address, taxpayer identifier, and date of birth) although in some cases their employer may transmit that information to the bank or other financial institution on their behalf. In addition, the consumer is ultimately responsible for substantiation – that is, they must demonstrate to the IRS, if audited, that the funds were used for qualified medical expenses.

HRAs and health FSAs are a bookkeeping account of the group health plan sponsor. The plan sponsor establishes the accounts and will generally partner with a financial institution or administrative services provider to administer the account. The plan sponsor is responsible for determining whether the funds are used for qualified medical expenses (and in some cases may limit the types of expenses such as only permitting reimbursement for dental or vision care). As noted, the plan sponsor determines if money in the account is rolled-over at the end of the plan year and generally will keep any unspent funds when the individual leaves employment. In the case of the HRA, the employer also provides health coverage through insurance or a self-funded group health plan.

State and Federal Privacy and Data Security Protections

The type of health care spending account and the respective roles of the health insurer, employer, and bank or other financial institution will determine which laws govern the collection, use, and disclosure of personal financial and health information. The chart below describes these relationships and applicable federal and state laws.

	Archer MSA	**HSA**	**HRA**	**Health FSA**
Who establishes the account?	Consumer (sometimes through employer)	Consumer (sometimes through employer)	Plan Sponsor	Plan Sponsor
Who owns information about account transactions?	Consumer	Consumer	Plan Sponsor	Plan Sponsor
What federal law applies?	Gramm-Leach-Bliley (GLB)	GLB	HIPAA/HITECH	HIPAA/HITECH
Is information used to administer the account PHI?	No	No	Yes	Yes
Is the insurer/group health plan a HIPAA covered entity?	Yes (for the HDHP)	Yes (for the HDHP)	Yes (for the HDHP) and the group health plan is a covered entity for the HRA.	The group health plan is a covered entity for the FSA.
Is the bank/financial institution a HIPAA business associate?	No	No	Yes – when processing PHI on behalf of the insurer/plan. Pure banking functions are exempt from HIPAA.	Yes - when processing PHI on behalf of the plan. Pure banking functions are exempt from HIPAA.
What bank agreements protect health information?	Data Protection Agreement with employer/plan sponsor	Data Protection Agreement with employer/plan sponsor	Business Associate Agreement with insurer/group health plan	Business Associate Agreement with group health plan
Who is responsible for providing notice of a data breach?	Bank	Bank	Insurer/group health plan	Group health plan

As you are aware, the Health Insurance Portability and Accountability Act established strong protections for the privacy and data security of protected health information (PHI). These standards were further strengthened by passage of the Health Information for Electronic and Technical Health (HITECH) Act in 2009. The federal statutes, and regulatory enforcement by the Department of Health and Human Services, set out restrictions on the collection, use, and disclosure of PHI, require covered entities to provide notice of how PHI is used and shared, and impose requirements for informing consumers if their information has been compromised.

The HIPAA and the HITECH Act apply to health insurers and group health plans offering health coverage in connection with a health care spending account. In addition, group health plans are subject the HIPAA and the HITECH Act when the plan provides employees with an HRA or health FSA.

Section 1179 of HIPAA exempts the application of privacy and data security standards to payment transactions by entities "engaged in activities of a financial institution" or "engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution . . . ." If the financial institution is using PHI on behalf of the group health plan for administering the HRA or health FSA, the bank is subject to HIPAA and the HITECH Act as a business associate.

In the case of Archer MSAs and HSAs the bank account is owned by the consumer and the bank is not subject HIPAA or the HITECH Act, but rather to privacy and data security standards established by the Gramm-Leach-Bliley (GLB) Act described below. While the bank or other custodian for the Archer MSA or HSA will typically have an extensive Data Protection Agreement with the employer, the account custodian is not considered a business associate under HIPAA.

GLB was enacted in 1999 and includes provisions governing the disclosure of nonpublic personal information which is defined in that Act as information that identifies an individual and is either (a) provided by a consumer to a financial institution; (b) results from any transaction with the consumer or service performed for the consumer or (c) is otherwise obtained by the financial institution. GLB applies to financial institutions that are custodians for Archer MSAs, HSAs, or where trusts are established, the HRAs, and health FSAs.

The Act establishes standards for how such information may be used and shared by banks and other financial institutions, requires consumers to be notified of the financial institution's practices for sharing information, and provides other protections for such information in the control of the bank or other financial institution. The bank or other financial institution is subject to significant regulation and oversight by federal banking authorities with respect to GLB compliance. These banking authorities have established comprehensive regulations governing how financial institutions may use and disclose information and conduct frequent audits of bank administration and operation of health care spending accounts and the security of information technology systems.

It is also worth noting the extensive state oversight of employers, health insurers, and financial institutions with respect to personal financial and health information. All jurisdictions have laws protecting health information maintained by or on behalf of health insurers – the state requirements typically mirror the federal HIPAA standards and in many cases state laws offer additional restrictions on the collection and use of "sensitive" health information such as personally identifiable data regarding treatments for behavioral health conditions, substance use disorders, abortion, and sexually transmitted diseases. In addition, 47 states and the District of Columbia have data breach laws governing information held by health insurers, financial institutions, and other businesses. These statutes typically require affected entities to notify consumers if their information has been wrongfully disclosed and impose penalties for data breaches.

Conclusion

AHIP appreciates the opportunity to provide testimony today regarding health care spending accounts and the privacy and data security standards that are applied to banks and other financial institutions – as well as to employers and health insurers – that establish and maintain these arrangements. These accounts – Archer MSAs, HSAs, HRAs, and health FSAs – provide consumers with flexibility in spending their health care dollars and the opportunity to save money for future medical expenses. Banks and other financial institutions, in partnership with employers and health insurers, are an important component in making these arrangements work for the benefit of consumers.

There is an extensive set of standards that have been established by states and the federal government to protect the personal financial and health information in these accounts. While HIPAA and the HITECH Acts apply to HRAs and health FSAs but not to Archer MSAs and

HSAs – we believe GLB as well as the existing state privacy and data breach requirements, provide the necessary and appropriate protections for consumer information.

NCVHS – Subcommittee on Privacy, Confidentiality & Security
HIPAA Section 1179

Tom Wilder
Senior Counsel
AHIP

Archer Medical Savings Accounts

- Established by HIPAA in 1996 – no new accounts after 2007.
- Small employer offers MSA along with qualified HDHP.
- Consumer sets up and owns bank account (employer may assist).
- HIPAA/HITECH applies to health insurer/group health plan HDHP.
- GLB applies to financial institution custodian of bank account.

Health Savings Account

- Established by MMA in 2003.
- Individual sets up bank account (employer may assist).
- Must be enrolled in qualified HDHP to contribute to account.
- HIPAA/HITECH applies to health insurer/group health plan HDHP.
- GLB applies to financial institution custodian of bank account.

Health Reimbursement Arrangement

- IRS guidance in 2002.
- Employer bookkeeping account – group health plan establishes HRA.
- Individual must be enrolled in group health plan coverage (insured/self-funded).
- HIPAA/HITECH applies to group health plan/insurer coverage.
- HIPAA/HITECH applies to group health plan HRA and to financial institution (as BA) if using PHI on behalf of group health plan.

Health Flexible Spending Account

- Employer bookkeeping account – group health plan establishes FSA through Section 125 plan.
- No requirement for other health coverage.
- Group health plan health FSA subject to HIPAA/HITECH.
- Financial institution subject to HIPAAHITECH (as BA) if using PHI for group health plan.