Sharing Data, Protecting Privacy: Potential Partnerships to Improve Benefits Access

September 2011

www.CenterforBenefits.org
About this Issue Brief

This Issue Brief explores the sharing of data among governmental human services agencies and between such agencies and community-based organizations that already play a vital role in helping eligible older adults and younger adults with disabilities access public benefits. This issue brief offers a preliminary exploration of how governmental entities can engage in data sharing with community-based organizations using authorities provided in the federal laws protecting the privacy of applicants. Using the example provided by the Medicare Improvements for Patients and Providers Act, it describes how in some states governmental agencies and community-based organizations have begun to use data sharing to streamline access to benefits such as the Part D Low-Income Subsidy (LIS, or Extra Help) and the Medicare Savings Programs (MSPs), two benefits that assist low-income Medicare beneficiaries in paying for their out-of-pocket Medicare-related costs.
Introduction

As states struggle to deliver services in a troubled fiscal climate, data-sharing agreements provide opportunities to increase efficiency by leveraging the networks of community-based organizations that already play a vital role in helping eligible older adults and younger adults with disabilities access benefits. Members of these vulnerable and often isolated populations trust and rely upon these organizations to provide accurate benefits information and comprehensive application assistance—including forms completion, assisting with gathering and submitting documents needed to verify eligibility, and troubleshooting. Data sharing has the potential to streamline the often daunting process of determining and recertifying eligibility for benefits. It can relieve the burden on state agencies by allowing staff to focus on adjudicating applications rather than engaging in the process of assuring appropriate applications completion and submission.

Government agencies that administer benefits such as Medicaid and the Supplemental Nutrition Assistance Program (SNAP, or Food Stamps) have long recognized the advantages of data sharing. In the course of determining applicants’ eligibility for and the amount of certain benefits, state agencies that have eligibility determination responsibilities share data with fellow state agencies (including the Department of Motor Vehicles) and with certain federal governmental agencies, such as the Social Security Administration (SSA), Centers for Medicare & Medicaid Services (CMS), and the Treasury Department. Yet few governmental entities have explored the potential efficiencies that may be achieved through sharing data for benefits access purposes with the community-based organizations that counsel older adults and younger adults with disabilities.

These governmental entities have valid concerns about protecting the integrity, privacy, and security of individually identifiable data. With appropriate procedures in place, however, governmental and non-governmental entities may share data with the consent or authorization of the individuals whose data are shared or upon entering into data-sharing agreements. Data sharing can lead to a more person-centered approach to benefits access for vulnerable older Americans and younger adults living with disabilities, while offering governmental agencies efficiencies in the administration of entitlement benefits.

This issue brief offers a preliminary exploration of how governmental entities can engage in data sharing with community-based organizations without violating the federal laws protecting the privacy of applicants. It addresses the two major federal privacy laws: the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Using the example provided by the Medicare Improvements for Patients and Providers Act (MIPPA) of 2008, we’ll describe how in some states governmental agencies and community-based organizations have begun to use data sharing to streamline access to benefits such as the Part D Low-Income Subsidy (LIS, or Extra Help) and the Medicare Savings Programs (MSPs), two benefits that assist low-income Medicare beneficiaries in paying for their out-of-pocket Medicare-related costs.

This brief focuses solely on privacy provisions—not security provisions. Future briefs in this series will explore how benefits access may be streamlined for eligible seniors and younger adults living

---

1 For the purposes of this issue brief, we define data sharing as the process by which an individual’s personally identifiable information, in the possession of a government agency, is shared for the purpose of applying for, recertifying, or verifying eligibility for a benefit, with a non-governmental organization that has assumed responsibility for assisting applicants with the process of completing applications or supplying required documentation needed to verify entitlement.
with disabilities, and applications processes made more efficient to save costs for governmental adjudications.

Data Sharing and Federal Law

Governmental entities have exhibited a historic reluctance to share data across agency jurisdictions, and even more with non-governmental benefits counseling organizations. Valid privacy and security concerns have limited the adoption of electronic data sharing for the purposes of benefits outreach and enrollment.

With the proper protections, data sharing is permitted and can streamline benefits access for those who are eligible, resulting in greater efficiency for administrative agencies. Organizations and agencies engaged in data sharing are required by law to implement systems and safeguards to protect the privacy of applicants’ personal information. Governmental entities may not share an applicant’s personal information without complying with federal and any applicable state privacy laws. Beyond the legalities, protecting applicant privacy ensures that potential beneficiaries feel confident that applying for benefits will not compromise their privacy. If applicants fear that their privacy would be violated through a data-sharing process, they may be discouraged from applying for the vital benefits for which they may be eligible.

Two key federal privacy protection laws—the Privacy Act of 1974 and HIPAA—establish the parameters of permissible data sharing. Neither the Privacy Act nor HIPAA contains any provision that would prevent governmental agencies from sharing health information with an outside organization for the purposes of enrollment in a government benefits program.

Privacy Act of 1974

The Privacy Act applies to the sharing of data that originates within the federal government with other governmental entities. In many ways, its aims and requirements are typical of most privacy laws. The Privacy Act was enacted to allow the federal government to hold and use individually identifiable information while also protecting individuals from unjustified violations of their privacy resulting from the government possessing their personal information. The most relevant protections of the Privacy Act limit sharing of individually identifiable information by the government. The statute creates a legal standard for the sharing of individually identifiable information among government agencies.

The Privacy Act generally requires an individual to consent prior to the sharing of that individual’s information by a federal agency. This requirement is intended to ensure that individuals are aware that the federal agencies possess a significant amount of individually identifiable information and that the information may be shared with their consent or pursuant to specific exemptions.

There are several exemptions to the consent requirement, most notably the “routine uses” exception. Routine uses are developed by federal agencies through the federal rulemaking process and authorize them to share individually identifiable information in certain circumstances. For example, a federal agency may share individually identifiable information with a contractor that is working for the federal agency. The use of federal data matching to determine or verify eligibility for public benefits is explicitly authorized by the Privacy Act. Agencies engaged in data matching must periodically inform applicants of such data-matching practices.

---

Consent provisions and recordkeeping requirements

When consent is required, the authorization to disclose personally identifiable information must include the general purpose for making the request and a description of to whom the information might be given. In addition, the agency collecting the information must keep a record of any information sharing that takes place, including what information was shared, and with whom.

In cases where an individual’s information has already been collected without a consent provision, it may be shared if a consent request, describing the use of the information and the recipient, is given to the subject of the information and returned with a signature. In general written consent is favored, although there are instances in which telephonic consent is permitted.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA created the first legally enforceable national standard to protect individually identifiable health information. The goal of HIPAA is to protect individual patients’ health information from unwarranted disclosure while at the same time ensuring that health information can be shared as needed to provide health care, and administer insurance and public health programs. A further purpose of HIPAA is to ensure that individuals may easily access their own health information.

HIPAA applies to the sharing of protected health information by entities within the healthcare system that obtain and share health information. Protected health information includes medical records, but extends beyond such records to include all information about an individual’s health that is or easily can be associated with a specific individual, such as information about a person’s physical or mental health conditions or status, as well as information about the delivery of health care or payment for health care and services. This broad definition encompasses information in the control of federal and state agencies that administer public benefits including Medicare and Medicaid.

Protected health information must be safeguarded from unauthorized disclosure by “covered entities” that include health plans, insurers (including governmental entities that administer public benefits), providers, and clearinghouses that share and match data between providers, insurers, and governmental overseers and administrators. HIPAA-covered entities are allowed to share protected health information for purposes related to treatment, payment, and health care operations as well as public interest and public benefit activities. State Medicaid agencies and the federal Medicare program are considered health plans for purposes of HIPAA and must adhere to HIPAA standards.

Requirements for authorized use of personal health information

All covered entities are permitted, and in some cases required, to share protected health information, but only if they comply with HIPAA’s requirements for such sharing. The basic HIPAA rule generally requires authorization from the individual whose health information is to be shared. The authorization requirements are more stringent, and the authorization to disclose includes, among other elements:

---

7 45 C.F.R. § 160.103 (2010).
8 45 C.F.R. § 164.508 (2010).
A description of the information to be shared.

The name of the person requesting the information.

The identification of the entity or person to which that information can be disclosed.

The intended uses of the information.

The signature of the person authorizing disclosure of her protected health information.

An expiration date.9

As with the Privacy Act, whatever protected health information is shared must be limited to the minimal amount of information required to accomplish the purpose of the sharing.10

While consent is the general requirement, HIPAA also identifies specific uses of personal health information that do not require notification of the individual whose information is to be shared. One such use is to enable government benefits programs to use protected health information to help determine eligibility.11

Exceptions for health oversight and benefits eligibility activities

For certain types of uses, such as the use of information for eligibility determination for government benefits programs, HIPAA-covered entities do not need to obtain authorizations to use or share protected health information. Instead, covered entities sharing protected health information are allowed to enter into business associate agreements with contractors who assist them with the benefit and eligibility determinations on their behalf. Under a business associate agreement, both the covered entity and the business associate are bound by the HIPAA privacy rules.12 For example, with such an agreement in place, a covered entity such as a state Medicaid agency may share protected health information with associates, such as MIPPA grantees, who voluntarily bind themselves to adhere to the HIPAA standards for enrollment and outreach purposes.

To comply with federal regulations, a business associate agreement must describe the permitted and required uses and disclosures of protected health information by the business associate. The business associate agreement must include a number of provisions. For example, the agreement must establish that the business associate will, among other things:

- Not use or further disclose the information other than as permitted or required by the contract or as required by law.
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract.
- Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware.
- Ensure that the same restrictions and conditions apply to any agents, including a subcontractor, to whom it provides protected health information for the purposes of performing the activities specified in the agreement.13

---

9 45 C.F.R. § 164.508(c) (2010). HIPAA-compliant authorizations must be in a plain-language written document that specifically references what information is to be disclosed, to and from whom, and for what purpose disclosure is requested. Authorizations must be signed and dated and must specify the duration of time within which disclosure is permitted.

10 45 C.F.R. § 164.514 (2010).


State Privacy Laws

Many states have enacted laws protecting privacy and the personal information of residents. State laws must comply with HIPAA, and may go beyond HIPAA to afford state residents additional privacy or greater access to their own health records. State laws may be stricter in protecting the privacy of health information, but are not allowed to enact more restrictive criteria than those contained in the HIPAA Privacy Rule that might expose protected health information to disclosures not allowed by the HIPAA Rule. Yet, while states may be stricter in protecting privacy and may offer their residents greater access to their own data, they cannot limit the effectiveness of the federal laws within their state.\(^{14}\)

Expanding Benefits Access while Protecting Privacy: MIPPA as Case Study

The implementation of the Medicare Improvements for Patients and Providers Act of 2008 provides a case study of data sharing among federal agencies, state agencies, and between these governmental human services agencies and community organizations. MIPPA illustrates how permissible data sharing could improve benefits access and promote program integrity by simplifying the benefits application process and to ensure that qualified seniors and younger adults living with disabilities apply for and receive the benefits for which they are eligible.\(^ {15}\)

Since the beginning of 2010, MIPPA Section 113 has required the Social Security Administration to transmit application data from LIS applicants to state Medicaid agencies to initiate an MSP application.\(^ {16}\) Once an individual has completed and submitted an LIS application (either on paper or online) their application is adjudicated by SSA. Verification of eligibility criteria occurs via data matching among federal agencies. In most cases applicants do not need to submit documents to prove their eligibility, as the data matching among federal agencies verifies all criteria.

Further, SSA shares LIS eligibility data with the Centers for Medicare & Medicaid Services which then assigns new LIS beneficiaries into Medicare Part D drug plans so they can use the drug coverage, which is only available through private drug plans.

Upon determining applicants’ eligibility for LIS, SSA transmits application data each weekday to state Medicaid agencies, regardless of whether the LIS application has been approved or denied. MIPPA requires that a state Medicaid agency treat these data as equivalent to an application for the MSP, with the receipt of data triggering the 45-day timeframe within which the agency must determine the applicant’s eligibility for benefits.\(^ {17}\)

Section 119 of MIPPA provides funding for LIS and MSP outreach and applications assistance to any state with a plan to engage its Area Agencies on Aging, State Health Insurance Assistance Programs, and Aging and Disability Resource Centers in this work.

---

\(^{14}\) Resources for researching privacy laws in your state can be found at the end of this issue brief.


Example of consent provisions and record-keeping requirements

The Social Security Administration obtains consent from LIS applicants to transmit LIS application data to state Medicaid agencies to trigger Medicare Savings Programs applications through an opt-out mechanism. The application for the Part D Low-Income Subsidy provides one example of a prior consent provision mandated by law. Question #15 of the application reads:

You may be able to get help from your state with your Medicare costs under the Medicare Savings Programs. To start your application process for the Medicare Savings Programs, Social Security will send information from this form to your state unless you tell us not to. If you want to get help from the Medicare Savings Programs, do not complete this question. Just sign and date the application and your state will contact you. If you are not interested in filing for the Medicare Savings Programs, place an “X” in the box below.

By checking the box, the applicant can opt out by declining to consent to the inter-agency data sharing under MIPPA. Applicants who leave the box blank are considered to have given their consent to SSA to share their data with the state Medicaid agency for the purposes of starting an application for the Medicare Savings Programs.

Example of exceptions to the HIPAA authorization requirement for health oversight and benefits eligibility

In some states that receive MIPPA funding, grantees have enhanced their activities by entering into business associate agreements, including data-sharing agreements, or Memoranda of Understanding, with their state Medicaid agency. The content of these agreements varies: in some states, the MIPPA grantee has full access to the database containing the applicant information transmitted to the Medicaid agency by SSA, but in others the grantee may have “read-only” access to the names and contact information of potential MSP applicants.

Through these agreements MIPPA grantees can better assist the Medicaid agency by helping potential beneficiaries complete their MSP applications, thereby making it more likely that the LIS data transmitted by SSA are converted into MSP enrollments. Through data-sharing agreements, MIPPA grantees reduce the burden on state Medicaid agencies, help them fulfill their mandate to increase enrollment in benefits programs, and increase the efficiency of the application and enrollment process.

---

Conclusion

While data sharing among government agencies and between governmental human services agencies and community-based organizations may not yet be the norm, data sharing holds tremendous promise to streamline access to benefits for seniors and younger adults living with disabilities while remaining within the bounds of federal and state law. State and federal governmental entities may increase the efficiency of their own eligibility adjudication processes, while also improving access to important benefits programs through bolstering their permissible use of data sharing.

MIPPA illustrates the potential benefits of intergovernmental data sharing to effect efficiencies while offering more person-centered benefits access. MIPPA also illustrates the potential gains of sharing data for benefits access purposes with appropriately trained community-based agencies that know how to protect the data and use it to efficiently perfect applications.

In the next issue brief in the series, we will provide examples of how MIPPA grantees have developed and implemented HIPAA-compliant data-sharing agreements with state Medicaid agencies so that they may gain access to the LIS applications data transmitted by SSA to their state Medicaid agency. We’ll review the mechanics of how MIPPA grantees were able to arrange to receive these data, and how they use them to efficiently complete and submit MSP applications for timely adjudication within the 45-day deadline. We’ll show how such practices improve access to MSPs for eligible applicants and to increase the number of low-income older adults and younger adults living with disabilities who are enrolled in this valuable benefit, which makes Medicare affordable for the poorest beneficiaries.
Resources


State Medical Records Laws: http://law.findlaw.com/state-laws/medical-records/.

About the Authors:

Lura Barber, MPP, is policy analyst and project manager and Hilary Sohmer Dalin is director, policy and programs at NCOA’s National Center for Benefits Outreach and Enrollment.

The authors would like to thank Jane Hyatt Thorpe, JD, Associate Research Professor, Department of Health Policy, School of Public Health and Health Services George Washington University and David Goldstein, former Summer Associate at NCOA, for their valuable contributions to this paper.
The National Center for Benefits Outreach and Enrollment

The National Center for Benefits Outreach and Enrollment (www.CenterforBenefits.org) helps organizations enroll seniors and younger adults with disabilities with limited means into the benefits programs for which they are eligible so that they can remain healthy and improve the quality of their lives.

The Center accomplishes its mission by:

- providing tools, resources and technology (such as www.BenefitsCheckUp.org) that help local, state and regional organizations to find, counsel and assist seniors and younger adults with disabilities to apply for and enroll in the benefits for which they may be eligible;
- generating and disseminating new knowledge about best practices and cost effective strategies for benefits outreach and enrollment; and
- funding and establishing Benefits Enrollment Centers in 20 areas of the country. Using web-based tools and person-centered approaches, these Centers help seniors in need and people with disabilities find and enroll in all the benefit programs for which they are eligible.

The Center is funded through a cooperative agreement with the U.S. Department of Health and Human Services’ Administration on Aging.