KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

PRIVACY AND SECURITY PROTECTIONS FOR PERSONAL INFORMATION IN CALIFORNIA'S HEALTH BENEFIT EXCHANGE

March 28, 2012

Under health reform, the federal government (and states at their option) will create exchanges to connect individuals and small businesses with affordable health insurance coverage and determine individual eligibility for public insurance programs and financial subsidies. These exchanges will collect, use and share personal information. Federal regulators have set baseline privacy and security rules to govern exchanges, but states are still required to develop specific privacy and security policies for their exchanges and ensure exchange compliance with other applicable privacy laws. This paper focuses on California's exchange, summarizing the federal and state privacy rules that apply and calling on state policymakers to develop a comprehensive framework of privacy and security policies to build and maintain public trust in the exchange.

The Patient Protection and Affordable Care Act of 2010 (PPACA), commonly referred to as health reform, authorizes the creation of health insurance exchanges, which will operate at the state and federal level, to help individuals find and enroll in affordable health insurance coverage.[1] The exchanges will also help small businesses secure health insurance coverage for their employees. Exchanges have the potential to improve access to health insurance for individuals who have customarily had difficulty finding or affording coverage. However, the information these exchanges will collect in order to perform their functions will be sensitive and must be protected by adequate privacy rules and security safeguards. Failure to provide privacy and security protections could jeopardize the public's willingness to take advantage of an insurance exchange's potential benefits.

Recently finalized federal regulations governing exchanges provide a strong foundation for the development and implementation of comprehensive privacy and security policies to protect personal information collected and shared by exchanges. However, states still must do the work of establishing workable and relevant policies that enable exchange operations while protecting personal data. California is well positioned to develop and implement policies from the outset that protect the privacy, confidentiality and security of personal information and promote public trust in the state's exchange.

This paper summarizes the federal rules that directly apply to California's exchange, explores whether other federal and state information privacy laws

[1] The Patient Protection and Affordable Care Act of 2010 (PPACA), Pub. L. No. 111-148, sec. 1311. The federal government will step in and operate an exchange for any state that fails to take action to establish its own by January 2013.

apply, and urges the state to work with consumers and other stakeholders to begin developing strong policies and best practices to govern information collected and shared by the state's exchange.

I. California's Health Benefit Exchange

The main purpose of insurance exchanges is to facilitate the purchase of health insurance by individuals and small businesses.[2] PPACA establishes some requirements for state health insurance exchanges (see below) but leaves considerable flexibility to states to define exchange functions and create the exchange infrastructure. Under PPACA, a state exchange must begin operating by 2014, when individuals and small employers may begin using it to seek coverage. Exchanges may extend participation to large employers starting in 2017.

PPACA requires exchanges to perform the following core functions:

- Certify health plans that qualify under PPACA to participate in the exchange;
- Provide information to consumers;
- Facilitate purchase of health insurance and enrollment in government program; and
- Grant certifications exempting individuals from the requirement to obtain insurance.

In 2010, the California legislature adopted two bills - AB 1602 and SB 900 – that established the core functions of the state insurance exchange, the Health Benefit Exchange or HBEX.[3] See Appendix 1 for a more complete description of these two bills.

While the HBEX is still in the planning stages, the potential is great to create a system in California that dramatically simplifies applying for health insurance coverage and ensures that life events and changes in income do not mean loss of health benefits. If built and implemented correctly, consumers will no longer need to decide whether to apply for Medi-Cal, Healthy Families or private insurance. Instead, individuals will have a single, online portal at which a single application filed will be screened and result in the correct form of coverage and benefits depending on the applicant's circumstances. But it is also clear that HBEX operations will require new and unique exchanges of data among state agencies, the federal government, private health plans, businesses, individuals and the HBEX.

II. Federal PPACA Requirements Governing the HBEX

To function effectively, the HBEX will collect sensitive information, including, at a minimum, basic demographic information, financial information, immigration status,[4] incarceration status

[2] PPACA, Pub. L. § 1131(d)(4). See generally, Center for Medicare Services, Center for Consumer information and Insurance Oversight, Health Insurance Exchanges, http://cciio.cms.gov/programs/exchanges/index.html; The Kaiser Family Foundation, "Explaining Health Care Reform: What are Health Insurance Exchanges?" (May 2009) http://www.kff.org/healthreform/upload/7908.pdf.

[3] The California Health Benefit Exchange, California Department of Health Care Services, and Managed Risk Medical Insurance Board, collectively serving as Sponsoring Partners, plan to build Cal-HEERS, an information technology (IT) system that will serve as the consolidated IT support for eligibility, enrollment, and retention for the Exchange, Medi- Cal and Healthy Families. For ease of understanding, we refer to Cal-HEERS, its functions, and the HBEX administration collectively as the Health Benefit Exchange or HBEX. Accessed at www.healthexchange.ca.gov.

[4] The Small Business Exchange, or SHOP, will not collect this information.

and Social Security Numbers. Building and maintaining public trust in the HBEX requires the implementation of a comprehensive privacy and security policy framework that sets and enforces clear rules for the HBEX's collection, use, disclosure and retention of such personal information. Such a policy framework will build trust and increase the public's willingness to take advantage of the insurance exchange's potential benefits.

The PPACA statute places strong limits on what data can be collected about a person seeking insurance coverage through a health insurance exchange. Specifically under Section 1411 of the Act, data collection is limited "to the information strictly necessary to authenticate identity, determine eligibility, and determine the amount of the credit or reduction."[5] Section 1411 goes on to state that exchanges can use such information only "for the purpose of, and to the extent necessary in, ensuring the efficient operation of the exchange."[6] PPACA also limits the collection, use and disclosure of Social Security Numbers.[7] These numbers can only be required from applicants seeking health insurance benefits, not individuals simply exploring the exchange or comparing plans.[8]

The Department of Health and Human Services recently released final regulations for insurance exchanges.[9] The regulations include the following important privacy and security protections for personally identifiable information (PII)[10] collected and shared by the HBEX:

- Consistent with Section 1411 of PPACA, PII created or collected by the HBEX to perform the core functions may not be used or disclosed by the HBEX except to carry out those functions.[11] Any individual who knowingly or willfully violates this limitation may be subject to a civil penalty of not more than $25,000 per person or entity, in addition to any other penalties that might apply.[12]

- The HBEX must establish and implement privacy and security standards for PII that are consistent with the framework of fair information practices adopted by the HHS Office of the National Coordinator, the "Nationwide Privacy and Security Framework for the Electronic Exchange of Individually Identifiable Health Information."[13] Such policies and procedures must be in writing and available to the HHS Secretary upon

[5] PPACA, Pub. L. 111-148, § 1411(g)(1).

[6] *Id.* at § 1411(g)(2).

[7] *Id.* at § § 435.907(e)(1) and 155.305(f)(6).

[8] *Id.*

[9] Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers, 77 Fed. Reg. 18310 (Mar 27, 2012) (Amending 45 CFR § 155, 156, and 157). Accessed at http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/html/2012-6125.htm.

[10] The term 'personally identifiable information' is defined by reference to The Office of Management and Budget's Memorandum M-07-16. The memorandum defines PII as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The memorandum is available online at *www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.*

[11] 45 CFR § 155.260(a)(1).

[12] 45 CFR § 155.260(g).

[13] Office of the National Coordinator for Health Information Technology, The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, accessed at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173.

request, and identify any other applicable law governing the HBEX's collection, use and disclosure of PII.[14]

- The HBEX also must establish and implement operational, technical, administrative, and physical safeguards that will support compliance with privacy policies and limits on the HBEX's collection, use and disclosure of PII.[15]

- Sharing of PII between the HBEX and agencies administering Medi-Cal, California's Health Families Program, Access for Infants and Mothers for purposes of eligibility determinations must meet the privacy and security requirements set forth in the regulations, as well as requirements in other provisions of PPACA[16] and the Social Security Act.[17] In addition, agency-to-agency "data matching" programs also must comply with relevant federal rules.[18] Federal tax return information must also be kept confidential and used, disclosed, and maintained only in accordance with Section 6103 of the Internal Revenue Code (see Appendix 2 for additional details on the IRS requirements on federal tax information).[19]

- Except in circumstances where collection, use or disclosure of PII is required by law, or with respect to tax return information which is solely governed by Section 6103 of the Internal Revenue Code, the HBEX is required to bind contractors – such as Navigators, agents and brokers – and others accessing PII through an exchange to these privacy and security requirements. [20] The HBEX is also required to ensure its workforce complies with these requirements.[21]

The requirement on the HBEX to develop and implement written policies and procedures to implement specific fair information practice (FIPs) principles is key to ensuring that the protections are appropriate for the data flows necessary to support the operations of the exchange. According to the regulations, the HBEX will need to develop and implement policies that address the following FIPs:[22]

- Individual Access: Individuals should be provided with a simple and timely means to access and obtain their personally identifiable health information in a readable form and format;

[14] 45 CFR § 155.260(d).

[15] 45 CFR § 155.260(a)(4).

[16] Pub. L. 111-148, § 1413(c)(1) & (2).

[17] The HBEX must meet or exceed requirements set forth in Section 1942 of the Social Security Act. [45 CFR 155.260(e)(3)]

[18] Data matching agreements that meet the definition of "matching program" under 5 U.S.C. 552a(a)(8) must comply with 5 U.S.C. 522a(o).

[19] 45 CFR § 155.260(f).

[20] 45 CFR § 155.260(b).

[21] 45 CFR § 155.260(c).

[22] 45 CFR § 155.260(a)(3).

- Correction: Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied;

- Openness and Transparency: There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable health information;

- Individual Choice: Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their personally identifiable health information;

- Collection, use and disclosure limitations. Personally identifiable health information should be created, collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately;

- Data quality and integrity: Persons and entities should take reasonable steps to ensure that personally identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner;

- Safeguards: Personally identifiable health information should be protected with reasonable operational, administrative, technical and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and

- Accountability: These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be put in place to report and mitigate non-adherence and breaches.

With respect to the requirement to adopt security safeguards, the regulations provide further specificity and require the HBEX to ensure:

- The confidentiality, integrity, and availability of PII created, collected, used or disclosed by the HBEX;

- PII is only used or disclosed by those authorized to receive or view it;

- Tax return information is kept confidential pursuant to federal tax law;

- PII is protected against any reasonably anticipated threats or hazards to its confidentiality, integrity or availability;

- PII is protected against any reasonably anticipated uses or disclosures not permitted or required by law; and

- PII is securely destroyed or disposed of in an appropriate or reasonable manner and in accordance with retention schedules.[23]

The HBEX also is required to periodically assess and update security controls and specifically must develop and utilize secure electronic interfaces when sharing electronic PII.[24]

As noted above, the HBEX is required to adopt policies to address the issue of consent, and it is important that the HBEX Board consider what choices individuals will have with respect to information collected, used, or disclosed by the HBEX. However, overreliance on consent – and failing to comprehensively address the other FIPs – will result in weak privacy protection in practice.[25] In the case of the HBEX, individuals will be required to submit certain information (or to authorize the submission of information) necessary to secure coverage or determine eligibility for subsidies; if individuals want to use the HBEX to fulfill the individual mandate requirement, they will have no choice but to disclose the data requested by the HBEX. Consequently, it is important that the PPACA statute and regulations has set clear limits on what personal information can be collected by the HBEX and how it can be retained, used, and disclosed. In addition to the specific limitations discussed above, HHS made clear in the explanatory material accompanying the final regulations that exchanges may not use or disclose PII initially collected for eligibility determinations for marketing or fundraising purposes.[26]

The exchange regulations vest responsibility for developing privacy and security policies with the HBEX or another responsible state agency;[27] technology vendors tasked with operationalizing the HBEX are required to be bound by such policies if they handle PII.[28] Such vendor also should play a role in helping the HBEX and other relevant state agencies understand the technical capabilities that are available to support various policy choices.

Of note, HHS has committed to issuing further guidance for exchanges on a number of topics, including on development and implementation of privacy and security policies and protocols, notification in the event of a breach of PII, retention of PII, preventing fraudulent use of an exchange, and de-identifying data.

III. Applicability of Other Federal and State Data Privacy Laws

As noted above, federal regulations require exchanges, in their written privacy and security policies and protocols, to identify any other applicable law (beyond PPACA and laws expressly made applicable by PPACA to exchanges) governing the exchange's collection, use and

[23] 45 CFR § 155.260(a)(4).

[24] 45 CFR § 155.260(a)(5) & (6).

[25] Deven McGraw, *Rethinking the Role of Consent in Protecting Health Information Privacy,* The Center for Democracy and Technology (Jan. 26, 2009), http://cdt.org/paper/rethinking-role-consent-protecting-health-information-privacy.

[26] Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers, 77 Fed. Reg. 18310, 18341 (Mar 27, 2012) (Amending 45 CFR § 155, 156, and 157). Accessed at http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/html/2012-6125.htm.

[27] 45 CFR § 155.260.

[28] 45 CFR § 155.260(b).

disclosure of PII. The federal Privacy Act of 1974[29] and California's Information Practices Act[30] provide some additional protections for certain information collected or accessed by the HBEX, as summarized briefly below. The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) may apply to the HBEX if it takes on the functions of a covered entity. However, these laws would provide only a patchwork of protections that do not address the full complement of FIPs required to be addressed by the HBEX. Other state health data privacy laws, including the California Confidentiality of Medical Information Act and the Insurance Information and Privacy Protection Act, likely do not apply to the HBEX. A summary of this legal analysis is set forth below; details are available in Appendix 2.

The federal Privacy Act covers the flow of information between the federal government to the HBEX. The Act prevents federal agencies from disclosing information about an individual without their consent unless one of the exceptions is met.[31] The Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988, also regulates the use of computer matching[32] by federal agencies when records in one agency's system of records are matched with other federal, state, or local government records (these requirements have been highlighted in the HHS final regulations)[33]. Finally, the Privacy Act requires federal agencies to enact rules on how and when information can be released to state and local governments. Any information the HBEX collects from a federal agency or matches against a federal database will be subject to Privacy Act. As per the requirements of the Privacy Act, the Internal Revenue Service has a detailed set of requirements that control how federal tax information is shared with state governments, discussed in more detail in the Appendix.

California's Information Practices Act (IPA) regulates the collection and disclosure of personal information by state government agencies – thus, it applies to the HBEX.[34] The IPA has a detailed framework governing the collection of personal information,[35] with a focus on gathering personal information directly from the individual as often as possible and limiting information collected and maintained to only information which is relevant and necessary to accomplish a legitimate purpose of the agency.[36]

---

[29] For a detailed exploration of The Privacy Act, see the Appendix 2, Section 2.2. For a detailed exploration of the IRS Guidelines, see the Appendix 2, Section 2.3.

[30] For a detailed exploration of the Information Practices Act, see the Appendix 2, Section 2.4.

[31] 5 U.S.C. § 552.

[32] Under the Act, the term "matching program" means any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs. 5 U.S.C. § 552(o)(a)(8).

[33] According to 45 CFR § 155.260(e)(4) Data matching and sharing arrangements that facilitate the sharing of personally identifiable information between the Exchange and agencies administering Medicaid, CHIP or the BHP for the exchange of eligibility information that meet the definition of "matching program" under 5 USC 552a(a)(8), must comply with 5 USC 552a(o).

[34] The term "agency" means every state office, officer, department, division, bureau, board, commission, or other state agency. It does not apply to the State Compensation Insurance Fund. Neither does the IPA apply to city or county agencies. Cal. Civ. Code § 1798.

[35] Cal. Civ. Code § 1798.14.

[36] *Id.*

Of note, the IPA sets different (and potentially stricter) standards for sharing of information between or among agencies versus sharing of information within a single agency. Section 24(e) authorizes disclosure or transfer of information to another state agency if the transfer is "necessary" to the second agency's duties and the use by that second agency is "compatible" with the original collection purpose. Section 24(d) authorizes the disclosure of information within an agency if the disclosure is "relevant and necessary" to the new user's duties and is "related" to the purpose for which the information was initially acquired. Because the HBEX will be operating as a stand-alone state entity, it will be subject to the potentially more stringent interagency guidelines when exchanging information with other agencies, including the Department of Public Health and the Department of Health Care Services. To ensure such interagency data sharing with the HBEX can occur, the uses by the HBEX will need to be viewed as "compatible" with purposes for which the information was collected by the originating agency. For example, information regarding an individual's incarceration status, collected and maintained by the California Department of Corrections and Rehabilitation, will need to be seen as "compatible" with the HBEX use of that information for eligibility determination purposes.

The explanatory material accompanying the PPACA final exchange rules discusses whether exchanges are either covered entities or business associates under HIPAA. Because states have flexibility in determining exchange operations beyond the core functions required by PPACA, coverage under HIPAA will depend on the exchange's actual activities. If the HBEX directly takes on a function that is characteristic of a covered entity (as defined in HIPAA regulations), the state may consider the exchange to be covered by HIPAA.[37] HHS notes as an example that a state "may need to consider whether the Exchange performs eligibility assessments for Medicaid and CHIP, based on MAGI, or conducts eligibility determinations for Medicaid and CHIP."[38] In the final rule, HHS provides no further guidance on this issue, other than to state that nothing in the final rule should be interpreted to create a business associate relationship between an exchange and a qualified health plan.[39] However, HHS does commit to releasing further guidance to assist states in determining the applicability of HIPAA and other federal laws to exchanges. Of note, HHS does acknowledge in the explanatory material to the final rule that HIPAA is "not broad enough to adequately protect the various types of PII that will be created, collected, used or disclosed by Exchanges and individuals or entities who have access to information created, collected, and used by Exchanges."[40] Thus, even if the HBEX is determined to be covered by the HIPAA regulations for some or all of its functions, the protections of HIPAA do not provide the type of limitations on data collection, use and disclosure required by PPACA. The HBEX Board will still need to establish a set of fair information practices-based policies to govern the unique operations of the HBEX.

Other federal and state health and personal information privacy laws, including the California Confidentiality of Medical Information Act[41] and the Insurance Information and Privacy

[37] Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers, 77 Fed. Reg. 18310, 18340 (Mar 27, 2012) (Amending 45 CFR § 155, 156, and 157). Accessed at http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/html/2012-6125.htm.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] For a detailed exploration of the California Confidentiality of Medical Information Act, see Appendix 2, Section 2.5.

Protection Act[42] likely do not apply (as explained in more detail in Appendix 2). Specifically extending them to apply to HBEX as a means of complying with PPACA will be insufficient, as those laws were enacted to respond to the information flow needs of specific entities in the health care system or in the financial sector and do not address the unique operations of the HBEX.

IV. Conclusion

Whether exchanges will realize their potential depends in substantial part on the extent to which consumers trust that data they store in and share via the HBEX is appropriately protected from misuse. To build trust in the HBEX, California must develop, implement and enforce specific policies that implement fair information practices and adhere to PPACA requirements. The HBEX and its board must act promptly, as the HBEX is being structured, to establish uniform and consistent confidentiality, privacy, and security policies and deploy technologies to appropriately protect personal health information.

In a subsequent paper, CDT - in conjunction with Consumer's Union - will discuss how to apply turn PPACA requirements into specific policies for the HBEX consistent with other applicable federal and California law.

For further information, contact Kate Black at kate@cdt.org or 415.882.1714.

[42] For a detailed exploration of the Insurance Information and Privacy Protection Act, see Appendix 2, Section 2.6.

APPENDIX 1

California's Health Benefit Exchange

In 2010, the California legislature adopted two bills - AB 1602 and SB 900 – that established the core functions of the state insurance exchange, the Health Benefit Exchange or HBEX. SB 900 focused on the organizational structure of the HBEX, with AB 1602 filling in the details on its operations.[43]

Pursuant to SB 900, the HBEX is an independent government entity not affiliated with any existing agency or department. The HBEX is run by a politically appointed Board with representatives of the governor, the Speaker of the California Assembly, the Senate Rules Committee and an ex officio member: the Secretary of Health and Human Services. Members of the Board serve four-year terms and must have demonstrated expertise in at least two of the following areas: the health care coverage market, the small group health care coverage market, health benefits plan administration, health care finance, administering a public or private health care delivery system, or health plan purchasing.[44] Members of the Board are not paid for their services.[45] The HBEX is headed by an Executive Director, serving at the pleasure of the Board, and run by a staff that is subject to limited civil service requirements, including conflict of interest protections.[46] The HBEX has been initially financed through federal grants and then, beginning in 2015, through fees imposed on participating health plans, at no point depending on state funds for operation or administration.[47]

AB 1602 assigns to the HBEX wide-ranging responsibilities on behalf of consumers and health plans. It requires the HBEX Board to establish requirements a health plan must meet in order to participate in the exchange as a "qualified health plan" and implement procedures for the certification, recertification, and decertification of such qualified health plans.[48] The selection of qualified plans must be done through a competitive process. The HBEX Board also is required to assess a reasonable charge on qualified plans.[49] AB 1602 further mandates that once qualified by the board, plans must use a standardized format and layout for presenting health benefits plan options, uniform billing and payment policies, and a uniform appeals process.[50]

---

[43] Cal. Senate Bill No. 900, §.2; Cal. Assembly Bill No. 1602; California Healthcare Foundation, Health Benefit Exchange: California vs. Federal Provisions, 2011, http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/H/PDF%20HealtHBEXnefitExchangeCAvsFederal.pdf.

[44] Cal. Senate Bill No. 900, § 2; California Healthcare Foundation, Health Benefit Exchange: California vs. Federal Provisions, 2011, http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/H/PDF%20HealthBenefitExchangeCAvsFederal.pdf.

[45] Cal. Senate Bill No. 900, § 2.

[46] *Id,* § 1(i).

[47] *Id,* § 2(k).

[48] Cal. Assembly Bill No. 1602.

[49] *Id.*

[50] *Id.*

The HBEX also will be an "active purchaser"[51] in the market of health plans – i.e., it will use market leverage and managed competition to negotiate product offerings with health insurers.[52] The HBEX will selectively contract for health care coverage for qualified individuals and qualified small businesses in the health insurance market; serve as an impartial source of information on health plans available in the market; provide structure to the market to enable consumers to compare health plans and purchase coverage; and serve as a broker of health insurance by handling premium billing and collection.[53] The HBEX also will enroll individuals in Medi-Cal and administer government subsidies for public health programs.[54] It has potentially broad powers to impact insurance options and benefits.

HBEX operations will require new and unique exchanges of data among state agencies, the federal government, private health plans, businesses, individuals and the HBEX. Many state agencies will need to operate seamlessly with California's exchange infrastructure, providing real-time, online eligibility determinations (under significantly reformed Medicaid income, asset, and eligibility rules).[55] Federal regulations call for real-time eligibility determinations that will rely on immigration status and income verification through a federal data services hub[56] that will obtain information from the Internal Revenue Service, the Department of Homeland Security and the Social Security Administration.[57] In addition, because PPACA provides new, refundable tax credits that will offset a portion of the cost of health insurance premiums, the HBEX must determine whether applicants are eligible for that advance payment of premium tax credits based on filing status and a number of other factors.[58] Further, the HBEX is required to notify the individual and individual's employer of an employee's eligibility for advance premium tax credits and cost-sharing reductions.[59] The HBEX will also have to check state and federal records to determine eligibility as well, as incarceration disqualifies an individual from HBEX eligibility unless it is "incarceration pending disposition of charges."[60]

---

[51] There are two archetypes in developing an exchange's organizational mode: "active purchaser" and "open marketplace." Active purchasing can include a range of activities. Some of the components of active purchasing are selective contracting, negotiating on price and quality, requiring payment and delivery reforms as part of plan design, requiring additional certifications, providing consumer education material. In an open marketplace exchange, on the other hand, any insurer can sell policies through the exchange as long as it meets certain minimum benefit requirements. Corlette, S. and J. Volk. 2011. "Active purchasing for health insurance exchanges: An analysis of options." Report for the Robert Wood Johnson Foundation, Georgetown University Health Policy Institute. pp. 22.

[52] *Id.*

[53] Cal. Assembly Bill No. 1602, § 8(a)(7)(c).

[54] *Id.* at § 8(a)(7).

[55] 45 C.F.R. §155.305(c).

[56] To ensure standardized service to Exchanges, Medicaid, and CHIP programs the federal Health and Human Services agency will establish a data services hub. Following the initial recommendations of the HIT Policy Committee adopted by the Secretary on September 17, 2010, HHS plans for the data services hub to verify citizenship, immigration, and tax information with the Social Security Administration (SSA), Department of Homeland Security (DHS), and Internal Revenue Service (IRS). Center for Medicare and Medicaid Services, *Guidance for Exchange and Medicaid Information Technology (IT) Systems, Version 2.0*, May 2011, accessed at *www.cciio.cms.gov/.../exchange_medicaid_it_guidance_05312011.pdf.*

[57] 45 C.F.R. §155.302, 45 C.F.R. §155.305(a).

[58] 45 C.F.R. §155.305(f)(2).

[59] 45 C.F.R. §155.310(h).

[60] 45 C.F.R. §155.305(a)(2), 45 C.F.R. §155.315(e). The term "pending disposition of charges" is not defined in the Regulation.

APPENDIX 2

A Detailed Analysis of Federal and State Privacy Law

2.1 The Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. HIPAA's Privacy Rule defines how covered entities[61] and their contractors or business associates may use and disclose identifiable personal health information (referred to in the Rule as protected health information or PHI). In general, covered entities may not use or disclose PHI without individual authorization – but there are many exceptions to the general rule, including allowing use and disclosure of PHI without consent for treatment, payment, and "health care operations." The Privacy Rule also requires covered entities to safeguard the PHI in their possession, and the HIPAA Security Rule sets forth specific security requirements for electronic PHI. The Privacy Rule also confers upon individuals certain rights with respect to their PHI, such as the right to request a copy of health information or to request that such information be amended if it is incorrect or disputed. In the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH),[62] Congress enacted a number of additional privacy protections, most of which are being implemented through amendments or additions to the HIPAA Privacy Rule.

HBEX will only be covered by the HIPAA privacy and security regulations if the state or the HHS Office of Civil Rights (OCR), which oversees those regulations, interprets exchanges to be covered. The term "covered entity" is defined by HIPAA to refer only to health care providers, health plans and health care clearinghouses, and each of those terms is specifically defined in the HIPAA statute.[63] The HBEX is clearly not a provider or clearinghouse (as explained in more detail below) but depending on its operations may fall under the definition of a health plan – or more specifically, one subcategory of health plan, a "health insurance issuer." A health insurance issuer is an "insurance company, insurance service, or insurance organization . . . that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance."[64] Although the HBEX could arguably be an "insurance service"—because it provides a service by which people can purchase health insurance—there are a number of conflicts between the statutory definition of an "insurance issuer" and the role of the HBEX. The PPACA vision of an exchange is a government agency or quasi-government organization that *facilitates* the purchasing of qualified health plans by individuals and small groups. [65]Under PPACA, exchanges are neither required nor expressly authorized to engage in the business of insurance, although the statute does not prohibit this function. Further, neither AB 1602 nor SB

[61] A covered entity under HIPPA can be 1) a *health plan*, 2) a *health care clearinghouse*, or 3) a *health care provider* who transmits any health information in electronic form in connection with a HIPAA covered transaction. 45 CFR 160.103.

[62] HITECH was enacted as part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.

[63] 45 CFR § 160.103.

[64] *Id*.

[65] Pub. L. No. 111-148, § 1311(b)(1); CMS & CCIIO, Initial Guidance to States on Health Insurance Exchanges, available at http://cciio.cms.gov/resources/files/guidance_to_states_on_exchanges.html.

900 require, prohibit or make reference to the HBEX engaging in the business of insurance. However, if HBEX operations were structured to include actually issuing insurance policies, it would likely meet the definition of a health plan and be covered by HIPAA.

Further, while OCR considers Medicare and Medicaid to be covered as health plans, because they are government programs that pay for health care and bear risk for health care costs,[66] it is unclear the HBEX will be seen as playing a similar role. The HBEX's website indicates, "the Exchange does not change how existing state health care coverage programs are administered." Instead, it will "screen and enroll" individuals and coordinate with other agencies to facilitate transition if and when an individual's eligibility changes.[67] Based on this description, it appears that the HBEX is not currently contemplating bearing risk for or directly paying for health care costs. Similarly, the HBEX may directly pay or facilitate the payment of federal tax credits for the purpose of offsetting premiums under PPACA. If such is the case, the HBEX may be considered a health plan because it will be a government funded program paying for the cost of health care.[68]

As noted above, it is unlikely that OCR or a state will consider exchanges to be health care clearinghouses, which are entities that process health information into standard data elements.[69] The HBEX will be an aggregator of health benefit plan information, which it will then reproduce for consumers seeking to enroll in health coverage. In helping to match the consumer with an appropriate plan, the HBEX will collect personal information from the consumer, but the function of an HBEX is not to perform the data standardization functions that are characteristic of a clearinghouse.

OCR might consider the HBEX to be a "business associate" under the Privacy Rule; although it is far from clear that designation makes sense, and the text accompanying the PPACA exchange regulations seems to dismiss this possibility. A "business associate" is a person or entity who, "on behalf of a covered entity," "performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information."[70] The HBEX will perform some functions that benefit health plans, and health plans participating in the HBEX will be required to pay fees to the HBEX. But the HBEX will not be acting "on behalf of" the plans. It will primarily function on behalf of the consumer (and the State of California), and the fees paid by plans to the HBEX primarily support exchange functions that are for the benefit of the consumer (although those functions also support plans as well). This the approach HHS also followed in the final regulations, which state, "because the Exchange, in performing functions under §155.200, is not operating on behalf of a particular QHP issuer, but rather is

---

[66] For more information, see http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.

[67] www.healthexchange.ca.gov.

[68] See 42 U.S.C. 300gg-91(a) (2) and Department of Health and Human Services, Final Rule RIN 0938-AQ67, Provisions of the Proposed Regulation and Analysis and Responses to Public Comments, accessed at http://www.ofr.gov/OFRUpload/OFRData/2012-06125_PI.pdf. The rule is scheduled to be published in the Federal Register on March 27, 2012.

[69] According to 45 CFR 160.103, a health care clearinghouse is a public entity that either "(1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity."[69]

[70] 45 CFR 160.103. Examples in 45 CFR 160.103 include organizations that perform utilization review, quality assurance, data analysis, etc. In these examples, business associates typically do not have a relationship with the individual, although sometimes they do have contact, *e.g.* a billing agency.

acting on its own behalf in performing statutorily- required responsibilities to determine an individual's eligibility for enrollment in a QHP through the Exchange, it is not a HIPAA business associate of the QHP issuer in regard to its performance of these functions."[71]

However, the HBEX arguably plays a role analogous to independent insurance agents, which have generally been considered to be business associates.[72] Agents serve as intermediaries between employers or individuals seeking insurance coverage. Because agents are intermediaries, the relationship between the agent and the individual or small group can exist independent of any particular insurer. Also, to best serve their clients, agents ask for personal health information in order to match them with the most appropriate health benefit plans. While a contractual relationship might not exist between agents and an insurer, the agent facilitates the use of insurer or plan services by individuals or small groups. Consequently, the plan receives a benefit when an agent refers an individual or business to them. This benefit could be the basis for an interpretation that the agent works "on behalf of" the plan and is therefore a business associate.

OCR or California determines that the HBEX is a covered entity or business associate under HIPAA, the HBEX will be required by law to comply with HIPAA regulations. The final exchange regulations do make clear, however, that in such a case the HBEX would be required to comply with HIPAA and the more stringent and specific PPACA rules.

2.2 The Privacy Act of 1974

The Privacy Act of 1974 puts limits on the information collected and maintained about U.S. citizens and permanent residents by federal agencies.[73] Under the Privacy Act, agencies cannot disclose information about an individual without their consent unless one of the exceptions is met.[74] The Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988, also regulates the use of computer matching[75] by federal agencies when records in one agency's system of records are matched with other federal, state, or local government records.[76] It requires federal agencies involved in computer matching programs to negotiate written agreements[77] with the other agency or agencies participating in the matching

---

[71] Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers, 77 Fed. Reg. 18310, 18340 (Mar 27, 2012) (Amending 45 CFR § 155, 156, and 157). Accessed at http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/html/2012-6125.htm.

[72] Independent insurance agents are thought to be covered under HIPAA as business associates by many in the industry, even though they do not work on behalf of health plans or health care providers in the same way that a billing agency does. More information about insurance agents as business associates can be found in *Independent Insurance Agents & Brokers of America, Protecting Client Information Should be Important Priority for Agents and Brokers*, *available at* http://www.iiaba.net/.

[73] *The Privacy Act of 1974, 5 U.S.C. § 552(o).*

[74] *Id.*

[75] Under the Act, the term "matching program" means any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs. 5 U.S.C. § 552(o)(a)(8).

[76] 5 U.S.C. § 552(o)(e).

[77] The agreement can only last 18 months, though it can be renewed each year as long as it does not change. 5 U.S.C. § 552a(a)(o)(2)(c).

programs, obtain approval by the agencies' Data Integrity Boards[78] of the match agreements, furnish detailed reports about matching programs to Congress and OMB, notify applicants and beneficiaries that their records are subject to matching, and verify match findings before reducing, suspending, terminating, or denying an individual's benefits or payments.[79] The written interagency agreements have many requirements, including procedures for retention, destruction, duplication, re-disclosure, and use by receiving agencies.[80]

These requirements will apply to all information matched to a federal database by the HBEX and require that the HBEX develop and maintain use agreements with each federal agency that will supply matching records. Matching information about individuals to federal databases will be an important tool in improving the efficiency of the HBEX, and the Privacy Act provides important privacy and security protections for personal information matched between federal and state agencies, including income, Social Security Number, and public health plan enrollment verification. However, it's important to recognize that the Privacy Act only applies to federal agencies and is intended to limit federal agencies' use and disclosure of personal information. It does not apply directly to the HBEX and does not regulate any personal information collected by the HBEX from other state agencies or directly from individuals, nor does it directly limit HBEX uses and subsequent disclosures of information received from federal agencies. Further, the Privacy Act does not protect the personal information of those individuals who are not citizens or permanent residents of the U.S., Consequently, while the Privacy Act is an important protection; it covers only a narrow slice of the HBEX's collection, use, disclosure, and retention of personal information.

2.3 The Internal Revenue Code Section 6103

Section 6103 of the Internal Revenue Code is a confidentiality statute and generally prohibits the disclosure of federal tax information.[81] However, PPACA authorizes the disclosure of federal tax information to assist the HBEX in the eligibility determination process. As a condition of receiving tax information, the HBEX is required to show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Specifically, Section 6103 requires the receiving entity have safeguards in place designed to prevent unauthorized use, access, and disclosure and must ensure its safeguards will be ready for immediate implementation upon receipt of tax information.

---

[78] Every agency that uses a matching program must have a Data Integrity Board. This Board must consist of senior officials of the agency, including the Inspector General of the agency (if there is one) and any official selected to oversee Privacy Act compliance. 5 U.S.C. § 552(o)(u).

[79] 5 U.S.C. § 552(o)(a).

[80] Specifically, the written agreement must provide procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program; procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs; prohibitions on duplication and re-disclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program; and procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program. 5 U.S.C. § 552a(a)(8).

[81] 26 U.S.C. § 6103, Safeguards for Protecting Federal Tax Returns and Return Information, accessed at http://www.patentofficelawsuit.info/irs_6103.htm.

Section 6103 will apply to the HBEX and provides an important protection to personal tax information collected from the IRS by the HBEX. However, it only covers one small aspect of personal information collected, used, retained and disclosed by the HBEX.

2.4 California's Information Practices Act

In 1977 California adopted the Information Practices Act (IPA). The IPA was designed to accomplish three goals: place strict limitations on secondary use of information by state agencies; make state agencies accountable for their information practices; and increase individual awareness of the state government's personal information practices and policies.[82]

The IPA guards against the unauthorized disclosure of personal information by state agencies.[83] The statute broadly defines "personal information" as any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.[84] It includes statements made by, or attributed to, the individual.[85] The IPA has a detailed framework governing the collection of personal information,[86] with a focus on gathering personal information directly from the individual when possible and limiting information collected and maintained to only information that is relevant and necessary to accomplish a legitimate purpose of the agency.[87] Under the IPA, "no agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the information" meets one of the statute's exceptions.[88] Those exceptions are detailed and include allowing disclosure to the individual, to another with the individual's consent, or to another agency where the transfer is necessary for the transferee agency to perform its duties and the use is compatible with a purpose for which the information was collected.[89]

2.5 California's Confidentiality of Medical Information Act

The Confidentiality of Medical Information Act (CMIA) is California's primary health privacy statute. Like HIPAA, the CMIA generally prohibits the disclosure of a patient's personal health information by providers of healthcare, health care service plans, their contractors and certain other entities without that patient's prior authorization – but that requirement is subject to a number of exceptions. For example (and again, like HIPAA), an individual's personal health information may be disclosed for treatment, payment or operations without the need to obtain

---

[82] Greame Hancock, *California's Privacy Act: Controlling Government's Use of Information?*, 32 Stan. L. Rev. 1001, 1980.

[83] The term "agency" means every state office, officer, department, division, bureau, board, commission, or other state agency. It does not apply to the State Compensation Insurance Fund. Neither does the IPA apply to city or county agencies.

[84] Cal. Civ. Code § 1798.3.

[85] *Id.*

[71] *Id.*

[72] Cal. Civ. Code § 1798.14.

[88] *Cal. Civ. Code § 1798.24-1798.24b.*

[89] *Id.*

consent. The CMIA has 23 other exceptions allowing disclosure without consent, including a variety of legal process actions, law enforcement, public health, for quality assurance and licensing requirements, and for purposes of disease management.[90] Disclosures that do not qualify for one of these exemptions are governed by stringent requirements, including the need to obtain prior authorization.

But like HIPAA, the CMIA applies only to providers[91] of healthcare, health care service plans[92], their contractors[93], and any business organized for the purpose of maintaining medical information in order to make the information available to an individual.[94] As noted above, since the HBEX is a state agency, it doesn't qualify as one of the entities covered by the CMIA. However, some may argue that the HBEX qualifies or should qualify as a "health care service plan," which "arrange(s) for the provision of health care services to subscribers or enrollees."[95] But again, since the HBEX 's functions involve arranging for health insurance coverage and not arranging for health care services, the HBEX does not fit neatly into this definition. Some may seek to have the HBEX covered by the CMIA under the provision extending coverage to businesses "organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care."[96] However, this definition also is an ill fit for the HBEX, both due to its state agency status and the nature of its operations. While the HBEX likely will maintain some personal health information, its purpose in doing so is to facilitate the enrollment of individuals in insurance plans and not for the purpose of ongoing maintenance of that information. In addition, the information collected by the HBEX is not stored "in order to make it available to the individual." Instead, the information is entered for the HBEX's use in determining eligibility for coverage and potentially for subsidies. There may be an ancillary effect of making medical information available to an individual, but this is not the purpose of the HBEX.

2.6 California's Insurance Information and Privacy Protection Act

The Insurance Information and Privacy Protection Act (IIPPA) was enacted to create standards for the collection, use, and disclosure of information[97] gathered in connection with insurance

[90] Cal. Civ. Code § 56.10-56.17.

[91] A "provider" of health care under the CMIA (Cal. Civ. Code § 56.05j) refers to any person licensed or certified pursuant to the Business Professions Code, any person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act, any person certified pursuant to Division 2.5 of the Health and Safety Code; any clinic, health dispensary, or health facility licensed pursuant to Division 2 of the Health and Safety Code. A provider of health care does not include insurance institutions as defined in Section 79 of the Insurance Code.

[92] A "health care service plan" refers to any entity regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Cal. Civ. Code § 1345(f)). Under Knox-Keene, a health care service plan is either a person who undertakes to arrange for the provision of health care services to subscribers or enrollees, pay for or reimburse any part of the cost for those services in return for a prepaid or periodic charge paid by or on behalf of the subscribers or enrollees or any person…who solicits or contracts with a subscriber or enrollee in this state to pay for or reimburse any part of the cost of…the provision of health care services.

[93] A "contractor" under the CMIA (Cal. Civ. Code § 56.05(c)) is any person or entity that is a medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a health care service plan or provider of health care.

[94] Cal. Civ. Code §56.06(a).

[95] Cal. Civ. Code § 56.05(d).

[96] Cal. Civ. Code § 56.06(a).

[97] IIPPA covers "personal information" including "medical record information" that is gathered in connection with an insurance transaction. "Medical record information" is personal information that: (1) relates to an individual's physical

transactions[98] by insurance institutions, agents or insurance-support organizations.[99] IIPPA aims "to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices."[100] IIPPA provides a very stringent and detailed privacy framework.

Because the HBEX will be helping individuals find and enroll in health insurance coverage, the HBEX arguably falls into the category of an "insurance support organization" and therefore regulated by IIPPA. However, IIPPA exempts "government institutions" from coverage under its provisions, which likely includes government agencies.[101] Further, the HBEX arguably would not be covered under IIPPA because its purpose is not to support insurance companies but rather to support individuals and small businesses seeking to purchase insurance.

---

or mental condition, medical history or medical treatment, and (2) is obtained from a medical professional (including a pharmacist) or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian.# It does not apply to information that relates to or was collected in reasonable anticipation of a claim or civil or criminal proceeding concerning the individual.

[98] "Insurance transaction" means any transaction involving insurance primarily for personal, family, or household needs rather than business or professional needs that entails … the determination of an individual's eligibility for an insurance coverage, benefit, or payment.

[99] Insurance support organizations are defined as any organization that collect, receive, or maintain information in connection with insurance transactions which pertains to natural persons who are residents of this state, or, engage in insurance transactions with applicants, individuals, or policy holders who are residents of this state. The following shall not be considered "insurance-support organizations": agents, governmental institutions, insurance institutions, medical care institutions, medical professionals, and peer review committees. While governmental institutions are not defined by the Act, they are commonly defined as an established organization or foundation, especially one dedicated to education, public service, or culture run by government. Large organizations influential in the community, like a college, hospital, university, etc., are examples of government institutions.

[100] Cal. Civ. Code § 791.

[101] While IIPPA does not define "institutions," the common definition could understand an agency to be an institution. An institution is commonly defined as, "an organization, establishment, foundation, society, or the like, devoted to the promotion of a particular cause or program, especially one of a public, educational, or charitable character." (Definition accessed at http://dictionary.reference.com/browse/institution).