The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Permitted Uses and Disclosures: Exchange for Health Oversight Activities

45 Code of Federal Regulations (CFR) 164.512(d)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also regulates the circumstances in which CEs are permitted, but not required, to use and disclose PHI to others for certain activities *without first obtaining* an individual's authorization, including for **health oversight activities**. This fact sheet provides hypothetical scenarios of exchange between CEs and state and federal entities which involve permitted disclosures of PHI for **health oversight purposes**. Previous fact sheets have covered when a CE may share PHI for treatment, payment and health care operations, or in support of public health activities.

Other laws may apply. This fact sheet discusses only HIPAA.

Under HIPAA, a covered entity (or a business associate (BA) acting on its behalf) may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for oversight of the health care system, government benefit programs where health information is relevant to eligibility, or regulatory or civil rights law compliance where health information is necessary for determining such compliance.[1] In general, criminal investigative activities not related to health care fraud are treated as law enforcement activity and not health oversight.

A health oversight agency includes a federal, state, or local government agency authorized by law to oversee the public and private health care system or government programs in which health information is necessary for determining eligibility or compliance, or to enforce civil rights laws for which health information is relevant. The definition includes the employees, agents, contractors, persons or entities acting under a grant of authority of such public agency. (45 CFR 164.501)

Depending upon the nature and manner of a disclosure, other requirements of the HIPAA Privacy and Security Rules may be applicable. For example,

- Disclosures by a BA for health oversight activities must be consistent with the business associate agreement (BAA).
- Uses and disclosures for health care oversight activities also must comply with the minimum necessary provisions of the Privacy Rule (45 CFR 164.514). The discloser is permitted to reasonably rely on the health oversight agency's description of what the agency believes is necessary for its oversight purposes.
- All disclosures described in this fact sheet may be made electronically, so long as the transmission is compliant with the HIPAA Security Rule (45 CFR 164.302 et seq).
- For the permitted health oversight disclosures, the CE (or its BA) is not responsible under HIPAA for what the health oversight agency subsequently does with the information once information has been sent to it for a permissible reason and in a secure manner.

[1] 45 CFR 164.512(f)

- A health oversight agency is NOT the CE's BA so a BAA between the CE and the health oversight agency is neither required nor warranted.
- For verification purposes, a discloser may request that the health oversight agency supply a written statement on appropriate government letterhead, or other documentation of the health oversight agency's identity and authority.
- In addition, depending on the circumstances, certain disclosures permitted under the health oversight provisions may also be permitted under other provisions of the HIPAA Rules, such as those that permit disclosures required by law. Depending on the permission relied upon to disclose PHI, different conditions may apply.

Example 1: Exchange for Health Oversight of the Health Care System

Fact Pattern: Under the laws of State X, the Office of the Health Insurance Commissioner (OHIC) is a health oversight agency authorized to approve and oversee employer-sponsored group health plans in the state. As part of that oversight authority, OHIC evaluates conduct in the insurance market, including reviewing how claims are handled and other aspects of the insurers' operations. OHIC requests that the Model Company's health plan in State X provide claims data that includes PHI on their active health plan enrollees indicating for whom claims were processed and for what purpose.

Permitted Action: Pursuant to 45 CFR 164.512(d)(1)(i), Model Company's health plan may disclose PHI to OHIC for OHIC's health oversight activities.

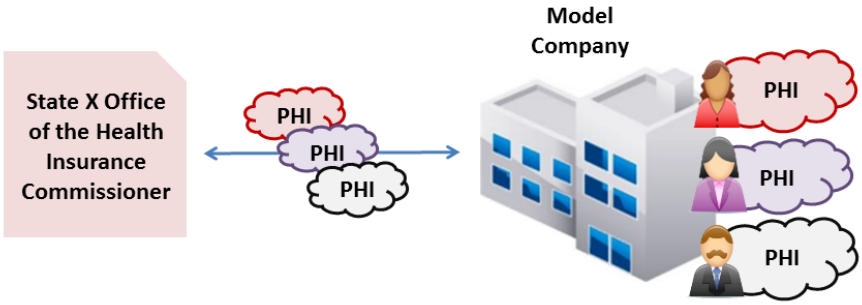

Figure 1: Health Oversight of the Health Care System Scenario

Example 2: Exchange for Health Oversight of the Health Care System

Fact Pattern: The State X Medical Board is a health oversight agency because it maintains oversight of health care provider licensees in the state. The Board asks Dr. Judy Smith, a state-licensed physician, for information to substantiate her compliance with state licensing requirements because it is investigating a series of related complaints against Dr. Smith by three patients.

Permitted Action: Under 45 CFR 164.512(d)(1)(i), Dr. Smith may disclose PHI to the Board for health oversight activities.

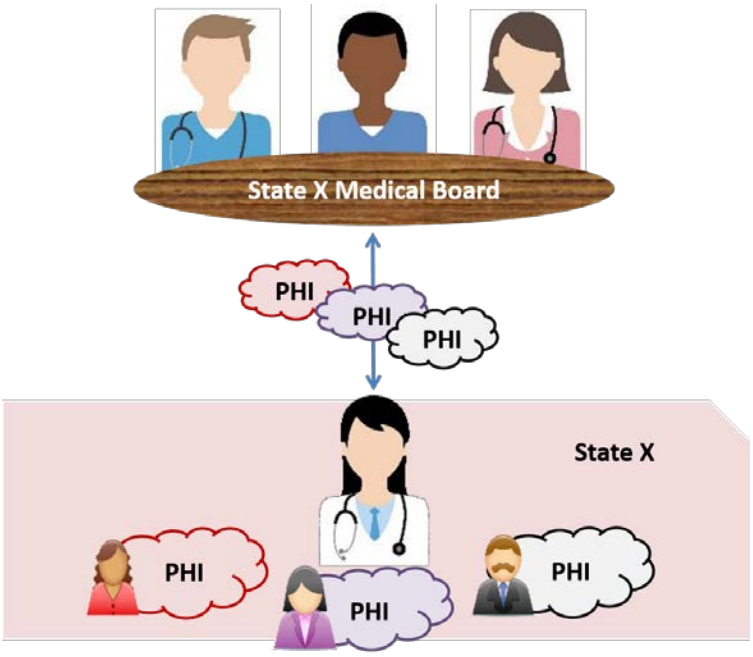

Figure 2: Health Oversight of the Health Care System Scenario

Example 3: Exchange for Government Benefits Programs

Fact Pattern: The Medicaid Fraud Control Unit in State X's State Attorneys General office has authority to conduct investigations of provider compliance with Medicaid requirements. State X's Medicaid Fraud Control Unit begins an investigation of Sunset Nursing Home to ensure its eligibility to be paid Medicaid funds following some consumer complaints. The Medicaid Fraud Control Unit requests information, including PHI, from Sunset Nursing Home.

Permitted Action: Under 45 CFR 164.512(d)(1)(ii), Sunset Nursing Home may disclose PHI to the Medicaid Fraud Control Unit for health oversight activities.

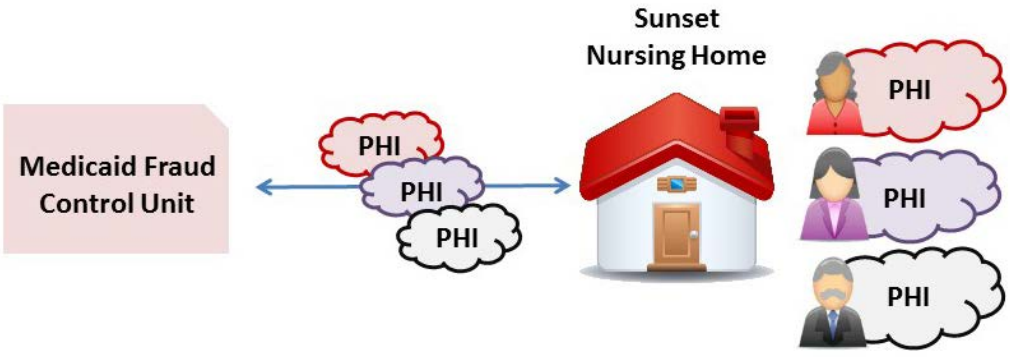

Figure 3: Government Benefits Programs Scenario

Example 4: Exchange for Entities Subject to Government Regulatory Programs

Fact Pattern: The U.S. Food and Drug Administration (FDA) is a health oversight agency of the federal government and requests PHI from Helpful Hospital to determine if certain implantable medical devices are causing harm to recipients.

Permitted Action: Under 45 CFR 164.512(d)(1)(iii), Helpful Hospital may disclose PHI to the FDA for health oversight activities that are within the FDA's authority.

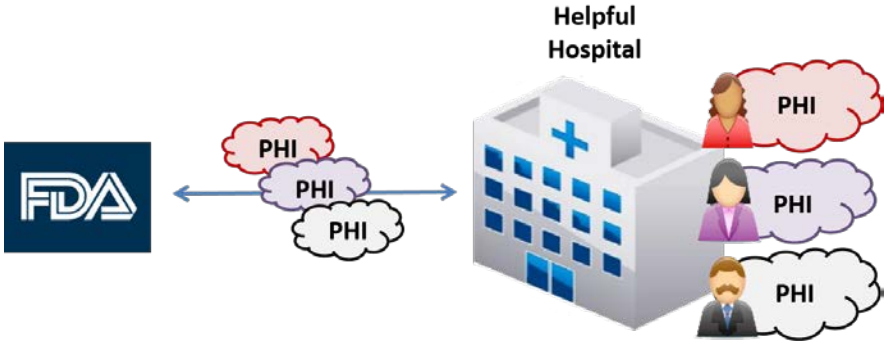

Figure 4: Government Regulatory Programs Scenario

Example 5: Exchange for Entities Subject to Civil Rights Law

Fact Pattern: A State Department of Insurance has authority to investigate whether Super Health Plan is complying with certain civil rights laws for which PHI is necessary to determine compliance. The State Department of Insurance conducts an audit about the civil rights compliance of Super Health Plan and requests information, including enrollee claims records that contain PHI.

Permitted Action: Under 45 CFR 164.512(d)(1)(iv), Super Health Insurance Company may disclose PHI to the State Department of Insurance for health oversight activities.

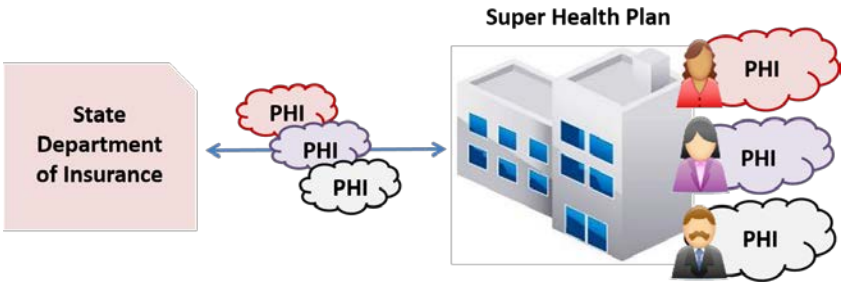

Figure 5: Civil Rights Law Scenario

Example 6: Exchange for Oversight – Requests from Medicaid contractors

Fact Pattern: The State of Good Health Medicaid Office is collaborating with contractors working for the U.S. Centers for Medicare & Medicaid Services (CMS) to collect data from providers for submission to CMS for Payment Error Rate Measurement (PERM) audits, which assess the occurrence of improper Medicaid payments and involve a review of claims paid by the State of Good Health Medicaid Office.

Permitted Action: Under 45 CFR 164.512(d)(1)(iii), providers may disclose PHI to CMS contractors directly, for health oversight activities, where the contractors are acting under a grant of authority from CMS to help determine compliance with Medicaid requirements, including payment review purposes.

Example 7: Exchange for Oversight - State Health Insurance Exchange

Fact Pattern: The State of Good Measures Health Insurance Exchange, which has oversight authority under state law over market conduct, operates a quality rating system which rates providers in part by using PHI in claims data from health plans participating in the Exchange. The Exchange requests that participating plans submit certain medical claims data on their patient enrollees to the Exchange's data contractor, to which the Exchange has granted oversight authority, to calculate ratings for providers.

Permitted Action: Under 45 CFR 164.512(d)(1)(i), plans may disclose PHI to the Exchange and its contractor for health oversight activities.

Using Certified Electronic Health Record Technology (CEHRT)

Providers who need to share PHI with health oversight agencies for health oversight purposes may use CEHRT to send the information to the requesting agency. Disclosure of ePHI by CEHRT or other electronic means requires HIPAA Security Rule compliance.

Additional Resources

- Office for Civil Rights HIPAA Regulations Website
- Office of the National Coordinator for Health Information Technology (ONC) Guide to Privacy & Security of Electronic Health Information (2015)[PDF-1.26MB]