FEDERAL PRIVACY BILL HITS COMP

June 16, 1998

by Eric J. Oxfeld

On April 2, S.1921, the Health Care Personal Information Nondisclosure (PIN) Act of 1998, was introduced by Senators Jim Jeffords (R-VT) and Christopher Dodd (D-CT). The Senate Labor and Human Resources Committee, which Jeffords chairs, has already held hearings and plans to continue work on the proposal. S.1921 does not directly refer to workers' compensation but will nevertheless increase "comp" costs.

S.1921 regulates the confidentiality of all personal health information (PHI), including records needed for workers' compensation purposes. Title I establishes safeguards to protect confidentiality; Title II requires the subject to authorize the release of PHI; Title III creates criminal and civil penalties for violation of the Act; and Title IV addresses the relationship to other laws and provides an effective date 18 months after enactment.

The safeguards apply to many entities who hold PHI, including doctors, employers, "health plans," and health insurers. These entities must allow the subject to copy and correct medical records. They must also provide notice of their confidentiality practices and apply "administrative, technical and physical safeguards to protect confidentiality, security, accuracy, and integrity" of PHI (all to be determined by federal regulation).

Employers must use the safeguards and are subject to sanctions, neither of which appear to cover *workers' compensation insurers* or *state workers' compensation administrative agencies*. However, employers, comp insurers, and workers' compensation agencies are all subject to the authorization process, under which doctors can release PHI to the employer or insurer only upon specific authorization from the subject. This authorization, which can be revoked at any time, preempts workers' compensation laws in most states, which currently do not require an authorization. PHI, when disclosed, must be limited to the minimum information necessary.

S.1921 creates 2 authorization tracks. A "health plan" can provide treatment, pay medical providers, and administer the plan, using one authorization signed at *enrollment*. Anyone else,

however, including workers' compensation, must use *two separate authorizations* collected by the doctor--one for the doctor's own use in treatment and reimbursement, and one for release to the insurer.

UWC believes privacy protections for workers injured on the job must be balanced against the legitimate need for prompt, accurate and complete medical information. We will continue working to strike an appropriate balance, but S.1921 as introduced falls short. Collecting multiple authorizations and allowing a claimant to revoke authorization for open claims could delay benefit delivery and drive up claim costs, especially if the employer or insurer cannot receive PHI showing that the claimant can return to work or has a lower degree of disability than claimed. Disputes over how much information is the "minimum necessary" and a private right of action that preempts state exclusive remedy provisions could give claimants leverage to drive up comp settlement values by threatening litigation over alleged privacy violations. These and other flaws must be fixed before **UWC** can support S.1921.

UWC is the only national business advocacy organization specializing exclusively in U.C. and workers' compensation issues.

STRATEGIC SERVICES ON UNEMPLOYMENT & WORKERS' COMPENSATION
1201 New York Avenue, N.W., Suite 750, Washington, D.C. 20005-6143
Phone (202) 682-1515 ❖ Fax (202) 842-2556 ❖ Email oxfelde@NAB.com

Summary of Federal Privacy Legislation - S.1921

prepared by Eric Oxfeld

May 6, 1998

Introduced April 2, 1998, by Senator Jim Jeffords (R-VT) and Christopher Dodd (D-CT)

Referred to Senate Labor & Human Resources Committee

§ 1 Short title

Health Care Personal Information Nondisclosure Act of 1998 (Health Care PIN Act)

§ 2 Findings

Individuals have a right of confidentiality with respect to their personal health information (PHI). This right is at risk. Consent is needed for disclosure except in "rare and limited circumstances required by the public interest." Disclosures should be limited to the minimum necessary. Incentives are needed to use non-PHI where appropriate. Timely and accurate PHI is needed for delivery of health care services, selected medical research, public health uses, and research on health outcomes and quality/efficiency of care.

§ 3 Purposes

Protect against unauthorized and inappropriate use of PHI created or maintained in connection with treatment, diagnosis, enrollment, payment, plan administration, testing, or research; promote efficiency and security in exchanging health information while protecting confidentiality; create incentives to use non-identifiable health information rather than PHI; provide remedies for violations.

§ 4 Definitions

Various terms, including but not limited to the following:

"Disclose" includes initial disclosure and subsequent redisclosure.

"*Employer*" means any employer as defined by ERISA with 2 or more employees.

"*Health care*" means "preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, ... counseling, service, or procedure - with respect to the physical or mental condition of an individual; or affecting the structure or function of the human body."

NOTE: Not clear whether this term covers *vocational* rehabilitation.

"*Health care operations*" means services by a "health plan" or medical provider to carry out "management functions" *of a medical provider or health plan*, including quality assurance and outcomes assessments; reviewing competence or qualifications of providers; accrediting; analysis of claims records; evaluating plan and provider performance; utilization review/pre-certification; underwriting and experience rating of health plans; and audits.

NOTE: HCO is limited by its terms to "health plans." Would HCO include *vocational* rehabilitation? Indemnity (cash) benefits?

"Health or life insurer" means a health insurance issuer as defined in the Internal Revenue Code § 9805(b)(2) or a life insurance company as defined in § 816.

"*Health oversight agency*" is [an entity that credentials providers]:
(i) a person who "performs or oversees an assessment, evaluation, determination or investigation" relating to the licensing/credentialing of providers, or
(ii) a public agency, person acting on behalf of a public agency, person acting pursuant to a requirement of a public agency, or person carrying out activities under federal or state law governing the assessment, evaluation, determination, investigation, or prosecution of an "audit, assessment, evaluation, determination or investigation" relating to the effectiveness of or compliance with or applicability of legal/fiscal/medical or scientific standards or aspects of performance related to the delivery of or payment for health care.

NOTE: HOA doesn't appear to include workers' compensation administrative agency.

"Health plan" means any health insurance plan including an HMO, or other program providing for or arranging for the provision of health benefits, whether or not funded through insurance.

NOTE: Workers' compensation does not provide "health benefits" and according to staff is not considered a "health plan."

"Health researcher" means a person who receives PHI as part of investigation to develop or contribute to "generalized scientific and clinical knowledge."

NOTE: Appears to be focused on medical research and thus would not include closed claims surveys used by WCRI, NCCI, and states.

"Law enforcement inquiry" means a lawful investigation by government into violation or failure to comply with criminal or civil law, regulations, rule or order.

"Payment" means activities by a health plan to determine coverage and actual payment under the plan, or by a provider to obtain payment for services. Includes billing, claim management, adjudication of health benefit claims, review of medical necessity and justification of charges.

"*Protected health information*" includes any personal information that relates to the past, present or future physical or mental health or condition of an individual (down to the cellular level); provision of care; or payment for care; created by a provider, health plan, researcher, health oversight agency, public health authority, employer, law enforcement official, health or life insurer.

"Public health authority" means a federal or state government unit that is "primarily" responsible for public health matters and "primarily" engaged in injury reporting, public health surveillance, and public health investigation or intervention.

NOTE: Appears to exclude workers' compensation administrative agency.

"*Secretary*" is the Secretary of HHS.

"*Treatment*" is the provision of care by, or coordination of health care among, providers, including referrals.

TITLE I – INDIVIDUAL'S RIGHTS

Subtitle A– Review of PHI by Subjects of the Information

§ 101 Inspection and Copying of PHI

(a) Provider, health plan, employer, health or life insurer, school or university shall permit subject of PHI to inspect and copy personal records.
(b) Exception by court order for (1) endangerment to life or safety of the subject; (2) revelation of confidential source; (3) information compiled for "civil, criminal, or administrative action or proceeding;" or (4) information compiled for clinical research authorized by an institutional review board and still under way.
(c), (d) Denial of request to inspect must be in writing, with reasons and procedures for appeal and opportunity to include subject's statement in the file.
(e) Inspection and copying of segregable portion of record.
(f) Deadline 30 days from request
(g) Agents of entities in subsection (a) must comply only where requested by the entity furnishing the records
(h) Nothing requires use of a "hearing."

§ 102 Amendment of PHI

Provider, health plan, employer, health or life insurer, school or university who holds PHI has 45 days to correct records at request of subject or give written explanation (subject to right to include subject's written statement in the records). Must make "reasonable" efforts to inform recipients in the chain of disclosure when records are amended. Exception for "repeated" requests for amendments. No requirement for hearing.

§ 103 Notice of Confidentiality Practices

Provider, health plan, *health oversight agency*, *public health authority*, employer, health or life insurer, *health researcher*, school or university shall post or provide written notice of confidentiality practices, including subject's rights, procedures to inspect/amend, etc.

Subtitle B – Establishment of Safeguards

§ 111 Establishment of Safeguards

Provider, health plan, *health oversight agency*, *public health authority*, employer, health or life insurer, *health researcher*, *law enforcement official*, school or university shall establish "administrative, technical and physical safeguards to protect confidentiality, security, accuracy, and integrity of PHI. Secretary may issue regulations to implement.

§ 112 Accounting for Disclosures

Provider, health plan, *health oversight agency, public health authority,* employer, health or life insurer, *health researcher, law enforcement official,* school or university shall keep records of disclosures in accordance with regulations issued by Secretary. Agent must keep records of its disclosures per §§ 205 through 212. Does not apply to officers or employees of recordholder who "have a need" for the PHI "in the performance of their duties." Record of disclosures must be maintained for 7 years.

TITLE II - RESTRICTIONS ON USE & DISCLOSURE

§ 201 General Rules

(a) Provider, health plan, *health oversight agency, public health authority,* employer, health or life insurer, *health researcher, law enforcement official,*, school or university may not disclose PHI except as authorized under this title.
(b) Entity in subsection (a) may use PHI internally pursuant to authorization under section 202 or 203 and consistent with limitations on disclosure in subsection (d). Disclosure to agent is considered internal use.
(c) Agent who receives PHI is subject to all rules of disclosure and safeguards.
(d) "Every disclosure of PHI by an entity under this title shall be limited to the information necessary to accomplish the purpose for which the information is disclosed."
(e) No requirement to disclose
(f) PHI must be identified as PHI when disclosed
(g) May disclose to employee or agent for sole purpose of creating non-identifiable information
(h) Manipulation of database of non-identifiable information to obtain identifiable PHI is a disclosure of PHI; disclosure of "anonymous link" which might be connected to prior disclosure to identify subject is disclosure of PHI.

§ 202 Authorization to disclose PHI for treatment, payment, or health care operations

(a)(1) To satisfy § 201, "single authorization form must be secured" for each individual in connection with treatment, payment and health care operations.
(2) Employer offering a health plan must obtain written authorization at time of enrollment with respect to PHI disclosed for treatment, payment, health care operations, *under the health plan.*
(3) Health plan itself must also obtain written authorization at time of enrollment.
(4) "Originating provider" whose care is delivered outside network or to uninsured individual must obtain written authorization to use PHI to provide or arrange care or seek reimbursement for medical services provided.

> NOTE: "Originating provider" is one who generates PHI. An IME would be included.

(5) Every provider providing care to an individual who hasn't previously provided authorization must obtain authorization concerning use and disclosure of PHI.

> NOTE: Appears to require that each successive "downstream" provider who generates new PHI must obtain separate authorizations to use and disclose.

(b) Authorization must identify the individual, describe the nature of the health care information to be disclosed, identify type of person to whom it will be disclosed, describe purpose of disclosure, state that authorization is revocable and valid until revoked, and be signed (may be electronic with unique identifier).

(c) Authorization provided under this section can be revoked unless the disclosure is required to effectuate payment for health care provided to an individual who hasn't agreed to pay for it personally. Authorization provided to a health plan is deemed revoked at cancellation or non-renewal of coverage, except as necessary to complete "health care operations and payment requirements related to the period of enrollment."

> NOTE: This doesn't appear to protect against revocation of disclosure required for purposes other than paying the provider for care, e.g., disclosure to effectuate payment of benefits to the individual, conduct an IME exam, etc.

(d) Record of authorization and revocation must be maintained for 7 years.

> NOTE: This provision is not limited to authorizations *under this section.*

(e) Authorization doesn't waive rights other federal or state laws, except as provided in this act.

> NOTE: This provision is not limited to authorizations *under this section.*

(f) Authorization to disclose PHI for treatment/payment/health care operations must be separate from any authorization to disclose to an individual with the intent to sell, transfer, or use PHI for commercial advantage (see § 203).

§ 203 Authorization to Disclose Other Than for Treatment/Payment/Health Care Operations

(a) Provider, health plan, *health oversight [agency], health researcher, public health authority, law enforcement official agency*, employer, health or life insurer, or school or university may disclose PHI other than for treatment/payment/health care operations only pursuant to a specific authorization separate from treatment/payment/health care operations authorization.
(b) Entity described in § 202 can't condition *delivery of treatment or payment for services* on receipt of authorization under this section.

> NOTE: This provision states that doctor can't refuse to provide treatment if patient won't authorize release of PHI for purposes other than treatment itself, payment of the doctor for the treatment, or health care operations under a health plan. Workers' compensation is not an entity described in §202, thus can an IME refuse to provide the exam if the worker won't agree to the authorization?

(c) Authorization under this section is revocable.
(d) Provider, health plan, *health oversight [agency], health researcher, public health authority, law enforcement official agency*, employer, health or life insurer, or school or university must provide PHI to coroner or medical examiner for use in inquiry into cause, manner and circumstances of death, without undue delay. Coroner must protect PHI.
(e) Recipient of PHI may use it only to carry out the purpose contained in the authorization.
(f) Secretary must develop model authorizations.

§ 204 Next of Kin & Directory Information

Provider may disclose PHI to next of kin or representative unless subject objects (or is incompetent and there are no prior indications of objection). The information must be limited to care currently being provided. Provider may disclose to anyone the individual's name, health status (e.g, critical, poor, fair,

etc.), or location, as long as location doesn't reveal specific information about the individual's physical or mental condition or there's reason to believe disclosure could lead to harm. Provider may release PHI as necessary to assist in identification or safe handling of deceased. Parent/guardian must act for minors under 14; minor or parent guardian can act for minors 14 through 17.

§ 205 Emergency

Any person who creates or receives PHI may disclose in emergency to protect health or safety of the individual from serious, imminent harm.

§ 206 Oversight

(a) Provider, health plan, employer, health or life insurer, *law enforcement official,* school or university may disclose PHI to health oversight agency for purposes authorized by law.
(b) Public health authority or health researcher may disclose PHI to health oversight agency for purposes of an oversight function of the public health authority authorized by law.
(c) Supervisor of oversight function must provide statement that PHI is sought for legal oversight function.
(d) PHI disclosed under this section can't be used against subject in administrative, civil or criminal action or investigation unless action/investigation arises out of and is directly related to *receipt of care or payment for care,* fraudulent claim, or oversight of public health authority or health researcher.

> NOTE: Receipt of care or payment for care appears to encompass an IME exam but not receipt or payment of indemnity (cash) benefits.

§ 207 Public Health

Provider, health plan, public health authority, employer, health or life insurer, *law enforcement official,* school or university may disclose PHI to public health authority or other person legally authorized by law for use in disease/injury report, public health surveillance, or public health investigation or intervention.

> NOTE: Is first and subsequent report of injury a "disease/injury report" to a "public health authority"?

§ 208 Health Research

Provider, health plan, public health authority, employer, health or life insurer, school or university may disclose PHI to health researcher if research is conducted or supported by federal agency, is a clinical investigation conducted pursuant to Food & Drug Administration rules, or is not subject to the "Federal Policy for the Protection of Human Subjects." Recipient of PHI under this section must remove individual identifier unless "institutional review board" approves; disclosure or use must be limited to the purposes of the research project or pursuant to §§ 205 and 206(b). Institutional review board must maintain appropriate records. Secretary has 3 years to report to Congress on institutional review boards. Secretary has 1 year to report to Senate Labor Committee on recommended standards to protect privacy in connection with research; final regulations are required with 2½ years unless Congress acts.

> NOTE: Closed claims surveys by WCRI or NCCI or state rating bureaus, or sponsored by state workers' compensation agencies or insurance departments, apparently would not be

"health research" under this section. Not clear whether the *initial* authorization to disclose PHI to workers' compensation insurer could extend to these legitimate uses of PHI under workers' compensation system.

§ 209 Disclosure in Civil, Judicial, Administrative Procedures

Provider, health plan, public health authority, employer, health or life insurer, *law enforcement official*, school or university may disclose PHI pursuant to discovery or subpoena in civil action in court, or request/subpoena in administrative proceeding, if made subject to court order. Court must determine lack of information would impair claim or defense. *Doesn't apply to party whose medical condition is at issue*, or when disclosure is allowed under §§ 202 - 208, 210, and 212. Doesn't supersede other grounds for objection to supplying information.

NOTE: Appears to require *court* order for use in resolving workers' compensation medical fee dispute unless there is valid authorization. Not clear what happens to a party whose medical condition *is* at issue.

§ 210 Law Enforcement

Provider, health plan, health oversight agency, employer, health or life insurer, school or university, or person receiving information under §§ 203 - 208 may disclose PHI pursuant to grand jury subpoena, administrative subpoena/summons/warrant, or request authorized under state or federal law. (Doesn't apply to disclosure to health oversight agency under § 206.) Law enforcement agency must show probable cause. Information must later be destroyed or returned, and redacted. Information obtained under this section may be used only for legitimate law enforcement purpose. PHI obtained without meeting these requirements can be excluded from evidence.

NOTE: Workers' compensation claims investigation or suspected fraud, or enforcement of law by workers' compensation administrative agency or insurance department, apparently is not encompassed in this definition, because "law enforcement inquiry" is limited to inquiry into a "violation."

§ 211 Postmarketing Adverse Experience with Drugs & Biological Products

Governed by FDA requirements.

§ 212 Payment Card and Electronic Payment Transactions

Recipient of payment may disclose PHI only as necessary to process payment/billing/collection. Credit card issuer or payment processor may use PHI only when necessary for processing payment, etc.

§ 213 Standards for Electronic Disclosures

Secretary must promulgate standards to disclose/authorize/authenticate PHI transmitted in electronic format.

§ 214 Individual Representatives

Agent/attorney/proxy may exercise rights of individual to extent so authorized. Person holding health care power of attorney may effectuate terms of grant of authority. Provider may disclose where

individual is incompetent and no one else (agent or next of kin, etc.) can be reasonably contacted. Act applies to deceased individuals for 2 years.

§ 215 Limited Liability for Law Enforcement Officers

No personal liability for violation unless intentional conduct with intent to sell/transfer/use PHI for commercial advantage, personal gain, or malicious purpose.

§ 216 No Common Law Liability for Permissible Disclosure

Provider, health plan, *health oversight agency, health researcher, public health authority*, employer, health or life insurer, *law enforcement official*, school or university who makes permissible disclosure has no common law liability.

TITLE III - SANCTIONS

Subtitle A–Criminal Provisions

§ 301 Wrongful Disclosure of PHI

Adds new chapter to federal criminal code for wrongful disclosure of PHI. Penalties are fine of $50,000, imprisonment up to 1 year, or both; $250,000/5 years if committed under false pretenses; $500,000/10 years and debarment from federal health care programs if committed with intent to sell/transfer/use for commercial advantage, personal gain, or malicious harm. Subsequent offenses double maximum penalty.

§ 302 Debarment

Provider, health researcher, health or life insurer, school or university may be debarred from federal health programs for violation.

Subtitle B–Civil Sanctions

§ 311 Civil Penalty

Noncompliance by provider, *health researcher,* health plan, *health oversight agency,* public health agency, employer, health or life insurer, *law enforcement agency,* school or university, or their agent, is subject to civil penalties, determined by the Secretary under this section (in addition to any other penalties). Violation of Title I – up to $500 for each violation, up to $5,000; Title II – up to $10,000 for each violation, up to $50,000; general business practice - up to $100,000.

§ 312 Civil Penalty Procedures

Secretary initiates; penalties may be recovered in civil action in the name of the United States. Injunctive relief authorized.

§ 313 Report on Existing Enforcement Mechanisms

Secretary reports to Congress regarding use of existing licensure, certification, and regulatory mechanisms including state insurance regulation, for imposition of sanctions.

§ 314 Private Right of Action

Authorizes civil action for knowing or negligent violation, including equitable relief and damages up to $5,000; authorizes punitive damages and payment of attorney fees and costs. Provides 3 year statute of limitations.

TITLE IV - MISCELLANEOUS

§ 401 Relationship to Other Laws; Veterans Benefits Exempt

Preempts state law directly related to the Act, but not federal laws relating to PHI or access to PHI. Preserves state law on privilege in *court*. Preserves state law on reporting vital statistics, abuse/neglect, and public or mental health laws restricting disclosures permitted under the act. Preserves laws authorizing collection/analysis/dissemination of information from provider, health plan, employer, health or life insurer, school or university when used for developing use, cost effectiveness, performance, or quality data. Secretary of Defense can issue regulations to protect national defense (parallel right for Secretary of Transportation with respect to Coast Guard).

> NOTE: Not clear whether state laws on privilege in workers' compensation administrative proceedings are preserved.

Limits on use and disclosure of PHI do not prevent any exchange of information within and among Department of Veterans Affairs to determine benefits for veterans.

§ 402 GAO study on research issues

Examination of research issues is due 6 months after enactment.

§ 403 Effective date

Effective 18 months after enactment. Regulations by Secretary are due 12 months after enactment.