GCD
Gardner Carton & Douglas

Paramore Consulting Inc.
e-commerce for healthcare

Permitted Disclosures

Under Gramm-Leach-Bliley and HIPAA

Overview of Case Study with Reusable Tools

Contents

Background

Health Insurance Portability and Accountability Act

Enacted in 1996, this federal Act has proven a catalyst for revolutionary change across the healthcare industry. Although initially focused on "portability" when an individual changes employment, HIPAA in its enacted form also contains several other provisions, most importantly the Administrative Simplification provisions. This section calls for standardization of electronic transactions and code sets; security of health information and electronic signatures; and privacy of all personally identifiable health information (PHI). The HIPAA Transaction Standards and Medical Codes final rule was put into effect in August 17, 2000, with a compliance deadline of October 17, 2002. In December 2000, the Department of Health and Human Services (DHHS) issued the final HIPAA privacy rules, and on April 14, 2001, President George W. Bush put them into effect. The compliance deadline for the privacy rule is April 14, 2003.

Among other things, this rule states that covered entities may not use or disclose PHI unless they have obtained the appropriate form of permission from the patient or the use or disclosure is expressly allowed by HIPAA. Entities covered by the HIPAA privacy rule include health care providers, payers, and clearinghouses.

Gramm-Leach-Bliley Act

Enacted in November 1999, the Gramm-Leach-Bliley Act (GLB) removed certain restrictions on mergers, affiliations and other business activities of banks and other financial institutions. Under GLB, previously barred affiliations between banks and insurers are now permitted. Concerned about the sharing of personal information among these affiliated entities, Congress added consumer privacy provisions to be enacted by each state insurance commissioner. The privacy provisions of Title V of GLB apply to non-public personal information and include personally identifiable financial and medical information.

Generally, GLB permits the sharing of virtually any information among affiliated entities. Covered entities will be required to provide notice of its information sharing practices and provide individuals with an opportunity to opt-out of certain types of disclosures before sharing personal information among its non-affiliated business partners.

Although HIPAA and GLB have several common requirements, specific GLB privacy protections will vary from state to state. Most states have enacted new laws and regulations

implementing GLB. Under many of these new laws, covered entities will be required to be in full compliance with GLB by July 1, 2001.

Overview of Case Study: Permitted Disclosures Under GLB and HIPAA

Paramore Consulting, Inc. (PCI) and Gardner, Carton & Douglas (GCD), working as an integrated team, brought together business consulting and legal analysis to conduct a privacy assessment and compliance project (the Project) for a large health plan located in the State of Virginia. The project involved analysis of the use and disclosure of protected information under both HIPAA and GLB, identification of areas of non-compliance and the development of compliance strategies relative to both laws.

The materials presented are based on those developed for the Project. It is important to note that the Project's initial focus was compliance with GLB due to its impending July 1, 2001 effective date. Because Virginia House Bill 2157 (HB 2157)[1], the Virginia version of GLB, prohibits certain disclosures without obtaining written authorization from the individual, disclosures were analyzed with particular emphasis on this requirement.

The secondary focus on the Project was compliance with HIPAA requirements. Uses and disclosures of protected information were categorized and underwent a high-level analysis. These efforts provide a solid baseline for a full HIPAA privacy gap analysis to be conducted after compliance with GLB is complete. The tools and models developed for the client can be used to facilitate its future HIPAA compliance efforts. These tools will support the maintenance of privacy compliance over time.

[1] Approved by the Governor on March 19, 2001, and enacted as 2001 Va. Acts ch. 371.

High Level Work Plan for Analysis of Permitted Disclosures

The overall business goal of this project was threefold:

- To create a detailed Uses and Disclosures Inventory;
- To provide health plan representatives with an understanding of its existing business practices and any gaps relative to HB 2157 and HIPAA Privacy mandates; and
- To provide health plan representatives with a detailed Privacy Risk Assessment for both HB 2157 and HIPAA.

Hundreds of documents and other information related to the health plan's uses and disclosures of protected information were collected, analyzed, and cataloged. Information flows were analyzed to identify disclosure practices. Specific disclosure practices and vendor relationships were identified for each business unit and for departments within business units.

Each disclosure practice was analyzed in light of the permitted disclosure citations within HB 2157 and HIPAA. The analysis keys are included herein and entitled GLB Permitted Disclosures Analysis Key and HIPAA Permitted Disclosures Analysis Key respectively.

PROJECT TIMELINE

The following timeline highlights tasks conducted over the course of an eight -week period.

Week 1: Documentation Discovery

A comprehensive effort to gather relevant policy and procedural documentation was completed. Hundreds of documents were reviewed and analyzed to determine if they contained protected information or led to its disclosure. Each document was indexed and cataloged for further analysis in the discovery of existing disclosure practices.

Weeks 2-4: Discovery through Facilitated Sessions and Interviews

Facilitated sessions and follow-up interviews allowed for the examination of the client's operational/business state. Products and services were mapped in business process and information flow charts. Internal information processing infrastructure was validated. Identification of external interfaces and their security and privacy controls also occurred during this component of the analysis. Using the information extracted via facilitated

sessions and follow-up interviews, a Uses and Disclosures Inventory was created. Analysis of safe harbor exemptions was also performed during this stage.

Weeks 5-6: Analysis

Analysis and critical thinking facilitated the identification of areas where the GLB Privacy and HIPAA Privacy requirements intersect during this stage of the project. This is also an appropriate time to evaluate the level of impact on business functions and degree of compliance or non-compliance.

Weeks 7-8: Reporting and Presentation of Findings

Findings were summarized and prioritized during this completion stage. Deliverable documents may include inventories of uses and disclosures with safe harbor indications, master document catalogs, and reference keys (samples included) and others described below.

The Uses & Disclosures Inventory (U&D) provides a detailed baseline of current practices across health plan business units. Through the various discovery and analysis methods employed, unique uses and disclosures in current practice were identified.

A Master Document Catalog was also compiled to contain data gathered from the physical inventory, review, and analysis of numerous individual documents and groups of documents submitted for the identification of its supported use, a disclosure, or neither. Data came from four (4) sources: document review, facilitated sessions, follow-up data collection forms, and interviews.

Finally, the findings of the Project were summarized in a detailed report. This report was covered under attorney-client privilege and distribution was strictly controlled. An Executive Summary presentation was prepared and delivered to the Chairman of the Board and senior management staff.

Key Concepts and Terminology

Throughout the conduct of this case study, several key concepts and "terms of art" were fundamental. The following examples demonstrate some of the most important areas for consideration while conducting such Privacy Analyses.

Information. The privacy section of GLB and the HIPAA Privacy Rule do not protect the same categories of information. In the case studied, HB 2157 protects 'privileged information' and 'personal information', while HIPAA covers 'protected health information'.

Uses and disclosures. The terms "use" and "disclosure" are not defined under GLB, however they are defined under HIPAA. Under HIPAA, 'Use' means the employment, application, utilization, examination, or analysis of protected information within an entity that maintains the information. 'Disclosure' means the release, transfer, provision of access to, or divulging in any other manner of protected information outside the entity holding the information. In short, 'use' occurs inside an entity, and 'disclosure' occurs outside an entity.

Identity as a Covered Entity. Understanding the identity of covered entities as it relates to GLB and HIPAA is critical to developing a compliance plan for permitted disclosures. The health plan owns several non-insurance affiliate companies and each business unit was examined to determine if it was a covered entity under GLB, HIPAA, both, or neither.

Analysis Keys

A number of automated and proprietary tools were utilized to assist in the organization and containment of all data catalogued during this project. Two versions of one of these tools are provided on the following pages in sample format. The "HB 2157 Permitted Disclosures Analysis Key "and "HIPAA Permitted Disclosures Analysis Key" were developed to allow for a line-item analysis of each disclosure in the Uses & Disclosures Inventory. The analysis of permitted disclosures was exception driven. If a disclosure fell into one of the permitted categories, then it did not require written authorization. If it did not (fall into one of the permitted categories), then a written authorization was required. Once the keys were developed, the line items were analyzed in a series of five passes allowing for review compared to HB 2157, HIPAA, separately first, and then together, with a final review including the health plans consideration.

HB 2157 Permitted Disclosures Analysis Key

An insurance institution, agent or insurance support organization may disclose personal[2] or privileged[3] information about an individual collected or received in connection with an insurance transaction, without written authorization under the following circumstances:

KEY	DESCRIPTION	CITATION	COMMENTS
A	To a person other than an insurance institution, agent or insurance support organization if the disclosure is reasonably necessary to enable that person to perform a business, professional or insurance function for the disclosing entity and that person agrees not to disclose the information further without the individual's written authorization unless the further disclosure:		
A1	Would otherwise be permitted if made by the disclosing entity	§ 38.2-613 (B)(1)(a)(1)	
A2	Is reasonably necessary for that person to perform its function for the disclosing entity	§ 38.2-613 (B)(1)(a)(2)	
A3	To enable that person to provide information to the disclosing entity for determining an individual's eligibility for an insurance benefit or payment	§ 38.2-613 (B)(1)(b)(1)	
A4	To enable that person to provide information to the disclosing entity for detecting or preventing criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with an insurance transaction	§ 38.2-613 (B)(1)(b)(2)	
B	To an insurance institution, agent or insurance-support organization, or self-insurer, if the information disclosed is limited to that which is reasonably necessary:	§ 38.2-613	
B1	To detect or prevent criminal activity, fraud, material misrepresentation or material nondisclosure in connection with insurance transactions	§ 38.2-613 (B)(2)(a)	

[2] "Personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. It includes an individual's name and address and medical-record information, but does not include privileged information or any information that is publicly available.

[3] "Privileged information" means any individually identifiable information that relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual and is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual.

KEY	DESCRIPTION	CITATION	COMMENTS
B2	For either the disclosing or receiving entity to perform its function in connection with an insurance transaction involving the individual	§ 38.2-613 (B)(2)(b)	
C1	To a medical-care institution or medical care professional for the purpose of verifying insurance coverage or benefits if only that information is disclosed as is reasonably necessary to accomplish the stated purpose	§ 38.2-613 (B)(3)(i)	
C2	To a medical-care institution or medical care professional for the purpose of informing an individual of an medical problem of which the individual may not be aware if only that information is disclosed as is reasonably necessary to accomplish the stated purpose	§ 38.2-613 (B)(3)(ii)	
C3	To a medical-care institution or medical care professional for the purpose of conducting an operations or services audit if only that information is disclosed as is reasonably necessary to accomplish the stated purpose	§ 38.2-613 (B)(3)(iii)	
D1	To an insurance regulatory authority	§ 38.2-613 (B)(4)	
E1	To a law enforcement or other government authority to protect the interests of the entity in preventing or prosecuting the perpetration of fraud upon it	§ 38.2-613 (B)(5)(a)	
E2	To a law enforcement or other government authority if the entity reasonably believes that illegal activities have been conducted by the individual	§ 38.2-613 (B)(5)(b)	
E3	To a law enforcement or other government authority upon written request of any law enforcement agency for information in the possession of the entity which relates to an ongoing criminal investigation	§ 38.2-613 (B)(5)(c)	
F	Otherwise permitted or required by law	§ 38.2-613 (B)(6)	
G	In response to a facially valid administrative or judicial order, including a search warrant or subpoena	§ 38.2-613 (B)(7)	
H	Made for the purpose of conducting actuarial or research studies	§ 38.2-613 (B)(8)	Provided that no individual is identified in a resulting report, materials allowing

KEY	DESCRIPTION	CITATION	COMMENTS
			individuals to be identified are returned or destroyed and the actuarial or research organization agrees not to disclose the information
I	To a party or a representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the entity	§ 38.2-613 (B)(9)	
J	To a non-affiliated third party whose only use of such information will be in connection with the marketing of a non-financial product or service	§ 38.2-613 (B)(10)	Provided that no medical record information is disclosed and the individual has been given the opportunity to opt out of the release of financial information and the receiving party agrees to use the information only for the stated purpose.
K	To a consumer reporting agency or from a consumer report reported by a consumer reporting agency	§ 38.2-613 (B)(11)	
L	To a group policyholder for the purpose of reporting claims experience or conducting an audit of the entity's operations or services	§ 38.2-613 (B)(12)	Provided the information disclosed is reasonably necessary for the group policyholder to conduct the review or audit.
M	To a professional peer review organization for the purpose of reviewing the service or conduct of a medical-care institution or medical professional	§ 38.2-613 (B)(13)	
N	To a governmental authority for the purpose of determining the individual's eligibility for health benefits for which the governmental authority may be liable	§ 38.2-613 (B)(14)	
O	To a certificate holder or policyholder for the purpose of providing information regarding the status of an insurance transaction	§ 38.2-613 (B)(15)	
P	To a lien holder, mortgagee, assignee, lessor or	§ 38.2-613	Provided that no

KEY	DESCRIPTION	CITATION	COMMENTS
	other person shown on the records of the entity as having a legal or beneficial interest in a policy of insurance, or to persons acting in a fiduciary or representative capacity on behalf of the individual	(B)(16)	medical record information is disclosed unless otherwise permitted and the information disclosed in limited to that which is reasonably necessary to permit such person to protect his interest in the policy.
Q	Necessary to effect, administer or enforce a transaction requested or authorized by the individual or in connection with servicing or processing an insurance product or service requested or authorized by the individual, or necessary for reinsurance purposes	§ 38.2-613 (B)(17)	
R	Pursuant to any federal HIPAA privacy rules	§ 38.2-613 (B)(18)	
S	An entity may disclose information about an individual collected or received in connection with an insurance transaction, without written authorization if the disclosure is:		
S1	To a nonaffiliated third party whose only use of the information will be to perform services for or functions on behalf of the insurance institution in connection with the marketing of the entity's product or service or the marketing of products or services offered pursuant to a joint marketing agreement	§ 38.2-613 (C)(1)	Provided that no medical-record information or privileged information is disclosed without the individual's written authorization unless otherwise permitted, the individual has been given notice and the opportunity to opt out of disclosure of financial information and the person receiving financial information agrees by contract, (i) not to use it except for the stated purposes and (ii) to maintain the confidentiality of the information unless otherwise permitted.

KEY	DESCRIPTION	CITATION	COMMENTS
S2	To an affiliate	§ 38.2-613 (C)(2)	Provided no medical record information or privileged information is disclosed without the individual's written authorization and the affiliate does not disclose the information except as otherwise permitted.

HIPAA Permitted Disclosures Analysis Key

Covered entities[4] can use Protected Health Information (PHI)[5] without consent or authorization if the purpose falls into one of three categories: treatment, payment, or healthcare operations. They may also do so under the conditions of § 164.512. These categories represent "permitted disclosures" for purposes of this analysis.

KEY	DESCRIPTION	CITATION	COMMENTS
P1	By a health plan to obtain premiums or to	§ 164.501 Payment (1)(i)	Payment By a health plan
P2	Determine or fulfill responsibility for coverages and provision of benefits under the health plan	§ 164.501 Payment (1)(i)	Payment By a health plan
P3	By a health care provider to obtain or provide reimbursement for the provision of health care	§ 164.501 Payment (1)(ii)	Payment By a health care provider
P4	The activities… relate to the individual to whom health care is provided and include, but are not limited to: Determinations of eligibility and coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims	§ 164.501 Payment (2)(i)	Payment
P5	Risk adjusting amounts based on enrollee health status and demographics	§ 164.501 Payment (2)(ii)	Payment
P6	Billing, claims management, collection activities, obtaining payments from reinsurance, and related health care data processing	§ 164.501 Payment (2)(iii)	Payment

[4] Health plans, health care providers, and clearinghouses are "covered entities".

[5] PHI is defined as individually identifiable health information maintained or transmitted orally, on paper, or in electronic format.
Information is "individually identifiable" if it permits identification of the individual or could reasonably be used to identify the individual.

KEY	DESCRIPTION	CITATION	COMMENTS
P7	Review of health care services, with respect to medical necessity, coverage, appropriateness of care, or justification of charges	§ 164.501 Payment (2)(iv)	Payment
P8	Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services	§ 164.501 Payment (2)(v)	Payment
P9	Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (A) Name and address; (B) Date of birth; (C.) Social Security Number; (D) Payment history; (E) Account number; and (F) Name and address of the health care provider and/or health plan.	§ 164.501 Payment (2)(vi)	Payment
T1	Provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to the patient; or referral of a patient for health care form one provider to another.	§ 164.501 Treatment	Treatment
H1	Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.	§ 164.501 Health Care Operations (1)	Health Care Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:

KEY	DESCRIPTION	CITATION	COMMENTS
H2	Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities	§ 164.501 Health Care Operations (2)	Health Care Operations
H3	Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 164.514(g) are met, if applicable	§ 164.501 Health Care Operations (3)	Health Care Operations
H4	Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs	§ 164.501 Health Care Operations (4)	Health Care Operations
H5	Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies	§ 164.501 Health Care Operations (5)	Health Care Operations
H6	Business management and general administrative activities of the entity including, but not limited to:	§ 164.501 Health Care Operations (6)	Health Care Operations
H7	Management activities relating to implementation of and compliance with the requirements of this subchapter	§ 164.501 Health Care Operations (6)(i)	Health Care Operations
H8	Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer	§ 164.501 Health Care Operations (6)(ii)	Health Care Operations

KEY	DESCRIPTION	CITATION	COMMENTS
H9	Resolution of internal grievances	§ 164.501 Health Care Operations (6)(iii)	Health Care Operations
H10	Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity	§ 164.501 Health Care Operations (6)(iv)	Health Care Operations
H11	Consistent with the applicable requirements of 164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in 164.514(e)(2).	§ 164.501 Health Care Operations (6)(v)	Health Care Operations
O1	Standard: Uses and disclosures required by law. A covered entity my use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.	§ 164.512 (a)(1)	Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.
O2	A covered entity must meet the requirements described in paragraph (c.), (e), or (f) of this section for uses or disclosures required by law.	§ 164.512 (a)(2)	

KEY	DESCRIPTION	CITATION	COMMENTS
O3	Standard: Uses and disclosures for public health activities. Permitted disclosures. A covered entity may disclose personal health information for the public health activities and purposes described in this paragraph to: A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;	§ 164.512 (b)(1)(i)	Permitted without authorization
O4	A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;	§ 164.512 (b)(1)(ii)	Permitted without authorization
O5	A person subject to the jurisdiction of the Food and Drug Administration;	§ 164.512 (b)(1)(iii)	Permitted without authorization
O6	To report adverse events (or similar reports with respect to food or dietary supplements), produce defects or problems (including problems with the use or labeling of a products), or biological product deviations if the disclosure is made to the person required or directed to report such information to the Food and Drug Administration;	§ 164.512 (b)(1)(iii)(A)	
O7	To track products if the disclosure sis made to a person required or directed by the Food and Drug Administration to track the product;	§ 164.512 (b)(1)(iii)(B)	
O8	To enable product recalls, repairs, or replacement (including locating and notifying the individuals who have received products of product recalls, withdrawals, or other problems); or	§ 164.512 (b)(1)(iii)(C)	
O9	To conduct post marketing surveillance to comply with requirement or at the direction of the Food and Drug Administration;	§ 164.512 (b)(1)(iii)(D)	

KEY	DESCRIPTION	CITATION	COMMENTS
NOTE:	MORE DETAILED CONDITIONS FOR THIS STANDARD CONTINUE IN THE REGULATION		STOPPED THE DETAIL IN THIS KEY FOR TIME SAKE.
O10	**Standard: Disclosures about victims of abuse, neglect or domestic violence**	§ 164.512 (c.)	Permitted without authorization
O11	**Standard: Uses and disclosures for health oversight activities**	§ 164.512 (d)	Permitted without authorization
O12	**Standard: Disclosures for judicial and administrative proceedings**	§ 164.512 (e)	Permitted without authorization
O13	**Standard: Disclosures for law enforcement purposes**	§ 164.512 (f)	Permitted without authorization
O14	**Standard: Uses and disclosures about decedents**	§ 164.512 (g)	Permitted without authorization
O15	**Standard: Uses and disclosures cadaveric organ, eye or tissue donation purposes**	§ 164.512 (h)	Permitted without authorization
O16	**Standard: Uses and disclosures for research purposes**	§ 164.512 (i)	Permitted without authorization
O17	**Standard: Uses and disclosures to avert a serious threat to health or safety**	§ 164.512 (j)	Permitted without authorization
O18	**Standard: Uses and disclosures for specialized government functions**	§ 164.512 (k)	Permitted without authorization
O19	**Standard: Disclosures for workers' compensation**	§ 164.512 (l)	Permitted without authorization

CH02/22130013.1