LGBT Bar
2019 Lavender Law Conference and Career Fair

Shhh It's a Secret (or Isn't It?):
Practical Ins and Outs of Health Care Privacy and Cybersecurity

CLE Materials

Cameron Faber
General Counsel
Los Angeles LGBT Center
cfaber@lalgbtcenter.org
(213) 993-7452

Greg Fosheim
Associate Attorney
McDermott Will & Emery LLP
gfosheim@mwe.com
(312) 984-7511

Sumaya Noush
Associate Attorney
Drinker Biddle & Reath LLP
Sumaya.Noush@dbr.com
(312) 569-1268

Colin Wright
Intellectual Property & Technology Counsel
Landis+Gyr
Colin.Wright@landisgyr.com
(678) 258-1412

Shhh It's a Secret (or Isn't It?):
Practical Ins and Outs of Health Care Privacy and Cybersecurity

Laws to protect health information privacy and confidentiality are largely designed to protect against the unauthorized access to, use of, and disclosure of personal health information. A variety of state and federal laws attempt to make health information secure from hackers, thieves, and rogue health care employees.

The individuals seeking disclosure from physicians might include law enforcement, public health authorities, relatives of the patient, employers, insurance companies, schools, and lawyers.

I. The Health Information Portability and Accountability Act

The Health Information Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 300gg, 300gg-1, and 300gg-2, enacted in 1996, contains a provision that required Congress to enact privacy legislation by August 21, 1999. If Congress failed to do so, the law directed the Secretary of Health and Human Services ("HHS") to promulgate regulations for the privacy of medical information. Following unsuccessful attempts to pass federal legislation, proposed regulations were issued in November 1999. After considering over 50,000 comments, the final regulations were issued on December 28, 2000, and had a compliance date of April 2003. The regulations appear at 45 C.F.R. Parts 160 and 164.

A. Who's Covered by the HIPAA Privacy Rule?

The HIPAA Privacy Rule (the "Privacy Rule") applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "Covered Entities").

Health care providers often assume they must comply with HIPAA; however, for many, HIPAA does not apply. If a health care provider does not submit electronic claims for reimbursement, that health care provider is most likely not subject to HIPAA. Massage therapists, estheticians, acupuncturists, naturopaths, and physicians who practice concierge medicine generally are not subject to HIPAA because they provide services that are not covered by a patient's insurance plan and thus, these providers do not submit claims electronically.[1]

A health plan includes health insurance companies, health maintenance organizations (HMO), governmental insurance (e.g., Medicare, Medicaid, Tricare), and employer-sponsored health plans. Self-insured companies with fewer than 50 employees may be exempt from HIPAA; however, we strongly recommend engaging experienced health care counsel if you have questions about HIPAA compliance for self-insured companies.

A health care clearinghouse is an independent third-party entity that forwards claims to payors after checking for errors and verifying that the information is compatible with the payor software and converting such information when necessary. The clearinghouse can also operate to return

[1] Note that state data privacy laws may still apply to any person or entity in possession of personally-identifiable information.

that information from the payor to the provider by re-converting it to the provider's preferred format.

B. What Information is Protected?

The Privacy Rule protects all individually identifiable health information held or transmitted by a Covered Entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" ("PHI").

C. Basic Principle for Uses and Disclosures

A primary purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by Covered Entities. A Covered Entity may not use or disclose PHI, except either (1) as the Privacy Rule permits, or (2) as the individual who is the subject of the information (or their personal representative) authorizes in writing.

D. Required Disclosures

A Covered Entity must disclose PHI in only two situations: (1) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI, and (2) to HHS when it is undertaking a compliance investigation or review or enforcement action.

E. Permitted Uses and Disclosures

A Covered Entity is permitted, but not required, to use and disclosure PHI, without an individual's authorization, for the following purposes or situations:

1. To the individual (unless required for access or accounting of disclosures);
2. Treatment, Payment, and Health Care Operations;
3. Opportunity to Agree or Object;
4. Incident to an otherwise permitted use and disclosure;
5. Public interest and Benefit Activities; and
6. Limited Data Set for purposes of research, public health, or health care operations.

Covered Entities may rely on professional ethics and best judgments to decide which of these permissive uses and disclosures to make.

F. Family and HIPAA

The HIPAA Privacy Rule contains several provisions that recognize the integral role that family members, such as spouses, often play in a patient's health care. For example, the Privacy Rule allows Covered Entities to share information about the patient's care with family members in various circumstances. It also generally requires Covered Entities to treat an individual's personal representative, who may be a spouse, as the individual, for purposes such as exercising the individual's rights under the Privacy Rule, including the right to access the individual's health information. In addition, the Privacy Rule provides protections against the use of genetic information about an individual, which also includes certain information about family members of the individual, for underwriting purposes.

The definition of *family member* in the Privacy Rule at 45 CFR 160.103 includes the terms *spouse* and *marriage*. The term *marriage* includes all lawful marriages. A lawful marriage is any marriage sanctioned by a state, territory, or a foreign jurisdiction as long as a U.S. jurisdiction would also recognize the marriage performed in the foreign jurisdiction. The term *spouse* includes all individuals who are in lawful marriages without regard to the sex of the individuals. The term *family member* includes lawful spouses and dependents of all lawful marriages. In addition, the terms *marriage*, *spouse*, and *family member* apply to all individuals who are legally married, regardless of where they live or receive health care services.

- The definition of a *family member* is relevant to the application of §164.510(b) regarding permitted uses and disclosures of PHI related to another person's involvement in an individual's care, and for making notifications about the individual's location, general condition, or death. Under certain circumstances, Covered Entities are permitted to share an individual's protected health information with a family member of the individual. Legally married spouses are family members for the purposes of applying this provision.
- The definition of a *family member* is also relevant to the application of §164.502(a)(5)(i) regarding the uses and disclosures of genetic information for underwriting purposes. This provision prohibits health plans, other than issuers of long-term care policies, from using or disclosing genetic information for underwriting purposes. For example, health plans may not use information regarding the genetic tests of a family member of the individual, or the manifestation of a disease or disorder in a family member of the individual, in making underwriting decisions about the individual. This includes the genetic tests of a lawful spouse of the individual, or the manifestation of a disease or disorder in the lawful spouse of the individual.

G. Personal Representative

Subject to limited exceptions, the Privacy Rule at 45 CFR 164.502(g) requires Covered Entities to treat an individual's *personal representative* as the individual with respect to uses and disclosures of the individual's protected health information and for purposes of exercising the individual's rights under the Privacy Rule. For example, a personal representative of an individual is able to review and obtain a copy of the individual's medical record or authorize disclosures of protected health information. In determining who is considered a personal representative, and thus able to act on behalf of an individual and exercise the individual's rights under HIPAA, the Privacy Rule generally looks to state laws governing which persons have authority to act on behalf of an individual in making decisions related to health care.

Under the Privacy Rule, if a state provides legally married spouses with health care decision making authority on behalf of one another, a Covered Entity is required to recognize the lawful spouse of an individual as the individual's personal representative without regard to the sex of the spouses.

OCR has issued a FAQ explaining that, under the HIPAA Privacy Rule, disclosures to a loved one who is not married to the patient or is not otherwise recognized as a relative of the patient under applicable law generally are permitted under the same circumstances and conditions as disclosures to a spouse or other person who is recognized as a relative under applicable law. The FAQ, while applicable in a variety of circumstances, was developed in large part to address confusion following the 2016 Orlando nightclub shooting about whether and when hospitals may share protected health information with patients' loved ones. The FAQ emphasizes that HIPAA does

not limit any permitted disclosures based on the sex or gender identity of the recipient of the information.

H. Authorized Uses

A Covered Entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. A Covered Entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in very limited circumstances.

Examples of disclosures that would require individual authorization include disclosures to a life insurer for coverage purposes, disclosure to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

I. Business Associates

The HIPAA Privacy Rule recognizes that health care providers and health plans cannot carry out all of their functions alone. Thus, covered entities are permitted to disclose protected health information to "business associates" upon obtaining satisfactory assurance that the business associate will use PHI only for the purposes for which it was engaged, will safeguard PHI from misuse, and will assist the covered entity with compliance with its duties when so required by the Privacy Rule.

Some examples of business associates are as follows:

- A third party claims processor that submits bills to insurance on behalf of a provider;
- A CPA that provides accounting services to a physician;
- A consultant who performs utilization reviews for a hospital;
- A healthcare clearinghouse that translates non-standard claims forms into a form that can be processed by a payor;
- Medical transcriptionists;
- Pharmacy benefits managers;
- **Attorneys who provide legal services to health care providers that may require access to PHI**.

Best practice is for a covered entity to enter into a Business Associate Agreement with a business associate. This agreement must contain all of the elements specified at 45 CFR § 164.504(e). A sample business associate agreement made available by the HHS Office of Civil Rights is attached as Appendix A.

A few common situations do not give rise to the need for a business associate agreement and PHI may be disclosed to the person or entity without the individual's authorization:

- Disclosures necessary for treatment of an individual;

    - Hospital may refer a patient to an outside specialist and transmit medical charts for treatment purposes without entering into a business associate agreement.
    - Physicians are not required to enter into business associate agreements with laboratories as a condition of disclosing PHI for the treatment of an individual.
    - Hospital laboratories do not need business associate agreements with outside reference laboratories for treatment of an individual.
- Disclosures to a health plan sponsor (such as an employer) by a group health plan, health insurance company, or HMO that provides benefits or coverage for the group health plan;
- Disclosures by a public benefit plan (e.g. Medicare) to another agency that is able to assist with determining eligibility or enrollment (e.g., Social Security Administration);
- Disclosures by a provider to a health plan for payment purposes;
- Persons in an organization (e.g., custodians; electricians) whose functions do not involve access to PHI and any encounters with PHI would be incidental;
- Conduits for PHI, such as postal workers and couriers;
- Between covered entities that participate in an Organize Health Care Arrangement as pertaining to disclosures that related to joint health care activities;
- When a group health plan purchases insurance from an insurance company or an HMO;
- When PHI is disclosed for research purposes, either with patient authorization, pursuant to a waiver, or as a limited data set; and
- Financial institutions processing funds for payment for health care or health plan premiums.

J. Minimum Necessary

A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A Covered Entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request. A Covered Entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a Covered Entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary rule is not imposed in the following circumstances:

1. Disclosure to or a request by a health care provider for treatment;
2. Disclosure to an individual who is the subject of the information (or their personal representative);
3. Use or disclosure made pursuant to an authorization;
4. Disclosure to HHS for complaint investigation, compliance review, or enforcement;
5. Use or disclosure that is required by law; or
6. Use or disclosure required for compliance with the HIPAA Transaction Rule or other HIPAA Administrative Simplification Rules.

K. Preemption

In general, state laws that are contrary to the Privacy Rule are preempted by the federal requirements. "Contrary" means it would be impossible for a Covered Entity to comply with both state and federal requirements, or that the provision of state law is an obstacle to accomplishing the full purposes and objectives of HIPAA. The Privacy Rule provides these exceptions to this general rule of federal preemption:

1. Relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information;
2. Provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or;
3. Require certain health plan reporting, such as for management or financial audits.

L. Enforcement and Noncompliance

The Privacy Rule provides processes for persons to file complaints with HHS, describes the responsibilities of Covered Entities to provide records and compliance reports and to cooperate with compliance reviews and investigations.

HHS may impose civil money penalties on a Covered Entity up to $50,000 per failure to comply with a Privacy Rule requirement, depending on the violation category, as described below. That penalty may not exceed $1.5 million per year for multiple violations of the identical Privacy Rule requirement in a calendar year. DOJ may impose criminal penalties depending on the severity and degree of scienter involved with non-compliance.

Civil monetary penalties

Tier	Penalty
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

Criminal penalties

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

M. Can individuals use HIPAA to bring a private action?

To-date, no federal court has found that HIPAA supports a private right of action. Recently, the District Court of the District of Columbia granted a defendant's motion to dismiss a suit that alleged the defendant failed to protect the plaintiff's privacy and confidentiality in violation of HIPAA. In Lee-Thomas v. LabCorp., the plaintiff alleged that the defendant's practice of entering medical information on a computer-intake station failed to properly shield her information from public view. The court granted the defendant's 12(b)(6) motion, stating that "the language of the [HIPAA] statute specifically limits enforcement action to HHS and individual states' attorneys general" (citing 42 U.S.C. §§ 1620d-5 to d-6 and citing several other district courts that dismissed private causes of action). (Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471 (DDC 2018)).

However, at least one state supreme court has held that non-compliance with HIPAA may be indicative of negligence and/or breach of contract under state data privacy provisions. In Byrne v. Avery, the Connecticut Supreme Court stated that "to the extent it has become the common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records pursuant to a subpoena." Under that framework, the court held that "a duty of confidentiality arises from the physician-patient relationship and that unauthorized disclosure of confidential information obtained in the course of that relationship for the purpose of treatment gives rise to a cause of action sounding in tort against the health care provider, unless the disclosure is otherwise allowed by law." (Byrne v. Avery Ctr. For Obstetrics & Gynecology, P.C., 327 Conn. 540 (2018)).[2] Whether HIPAA is a viable grounds for establishing a standard of care is yet to be determined and likely will depend on how state courts and legislatures establish privacy protections under state laws.

II. Distinguishing Genetic Privacy from General Notions of Medical Privacy

What makes genetic information different from other sensitive medical information? George J. Annas, world famous bioethicist, health care lawyer and policy advocate, is one of the leading academic voices in support in support of the argument that genetic information is more powerfully private than other types of information. It is information about us, but not just about us. It is information about our parents, siblings, and children. It is also information that is very important for private decision-making: who to marry, whether or not to have a child, whether or not to undergo prenatal testing, and the future health of your child. It is also information about our likely future health. All of our genetic information is contained in the nucleus of each one of our cells. So far, genetic exceptionalism has been criticized in peer-reviewed literature, but the approach has been adopted by legislatures where laws have generally addressed genetics separately from other health issues as uniquely private.

[2] An Ohio state court has also considered similar tort-based causes of action that used HIPAA as the standard of care. In Sheldon v. Kettering Health Network, the Ohio Court of Appeals held that HIPAA does not authorize a private right of action and "an administrative rule does not constitute negligence *per se*; however such a violation may be admissible as evidence of negligence." 40 N.E. 661, 674 (Ohio Ct. App. 2015).

The Genetic Information Nondiscrimination Act (GINA) was signed into law on May 21, 2008 by President George W. Bush. GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.

A. Health Coverage

The Department of Treasury, the Department of Labor, and the Department of Health and Human Services collectively promulgated regulations to implement Title I of GINA. (74 Fed. Reg. 51664, Oct. 7, 2009). Title I of GINA makes it unlawful for health insurers to request, require, or use genetic information to make decisions about:

- Your eligibility for health insurance
- Your health insurance premium, contribution amounts, or coverage terms

This means it is deny you coverage or determine your payment obligations based on a genetic test result or family history.

In addition, GINA prohibits your health insurer from:

- Considering family history or a genetic test result to be a pre-existing condition
- Requiring that you have a genetic test (or even asking you to do so)
- Using any genetic information to discriminate against you, even if they did not mean to collect it

Importantly, GINA does not prohibit health insurance companies from making coverage decisions based on your current health status, including manifestations of disease due to genetic factors. Rather, GINA prohibits discrimination based on a genetic predisposition to a disease that has not manifested. Once a person becomes symptomatic, GINA no longer offers protection. For example, an insurance company cannot raise premiums or deny coverage because a person has a positive genetic test for Huntington disease. However, once that person shows signs and symptoms and is diagnosed with the disease, then GINA does not prohibit insurance companies from using the diagnosis to make coverage determinations.

What health insurance does GINA protect?

GINA generally applies to health insurance that you receive through your employer or for health insurance that individuals purchase on their own. GINA also applies to Medicare and any insurance plans that are available to supplement Medicare beneficiaries' plans. GINA does not offer protection to individuals who obtain health insurance from the Indian Health Service, the Federal Employees Health Benefits Plans, or Tricare; nor does it protect against genetic information discrimination in other forms of insurance, such as life, disability, or long-term care insurance.

Can my insurance company require me to undergo genetic testing or request my test results?

Generally, insurers are prohibited from requesting or requiring genetic information about applicants or beneficiaries. The only exception to this generality is if genetic information is a key criterion for determining whether to pay for a requested test, treatment, or procedure in order to justify medical need. In such a situation, insurance companies must request only the minimum information necessary to make a determination, and any information that is received must not be further used to discriminate against a beneficiary.

B. Employment

GINA prohibits employers from using your genetic information in the following ways:

- To make decisions about hiring, firing, promotion, pay, privileges or terms
- To limit, segregate, classify, or otherwise mistreat an employee

This means it is unlawful for your employer to use family health history and genetic test results in making decisions about your employment.

It is also against the law for an employer to request, require, or purchase a potential or current employee's genetic information or that of his or her family members. There are a few exceptions to when an employer can legally have your genetic information. If an employer does have the genetic information of an employee, the employer must keep it confidential and in a separate medical file.

What is genetic information? (29 CFR 1635.3)

GINA defines genetic information to include the following:

- Your individual genetic tests;
- Your family members' genetic tests (including dependents and up to a fourth-degree relative);
- Family medical history or manifestation of diseases in family members;
- Any requests by an individual or a family member for genetic services or participation in clinical research studies that includes genetic services as part of the research;
- Genetic information of a fetus carried by an individual or a pregnant woman who is a family member of an individual; and
- Genetic information of any embryo legally held by an individual or a family member using assisted reproductive technology.

GINA does not include the following information:

- Sex;
- Age; or
- Information about race or ethnicity that is not derived from a genetic test, where "genetic test" is any test that assesses genotypes, mutations, or chromosomal changes

A 2012 case from Virginia is illustrative regarding genetic information. The plaintiff alleged that he was terminated from his employment in part because he disclosed his wife's multiple sclerosis diagnosis and prognosis on a health insurance questionnaire regarding his family's general medical conditions and medications. A month later, an office manager asked when his wife was diagnosed and about her prognosis. Three days later, the plaintiff was terminated without explanation. Addressing the plaintiff's GINA claims, the Western District of Virginia clarified that "a consistent history of an inheritable disease in an individual's family may be viewed to indicate that the individual himself is at an increased risk for that disease; [h]owever, the fact that an individual family member merely has been diagnosed with a disease or disorder is not considered 'genetic information' if 'such information is taken into account only with respect to the individual in which such disease or disorder occurs and not as genetic information with respect to any other individual'." Poore v. Peterbilt of Bristol, LLC, 852 F. Supp. 2d 727, 731 (W.D. Va. 2012) (quoting 2008 U.S.C.C.A.N 101, 105-106). The court explained that the plaintiff may have a claim under the Americans with Disabilities Act, but to state a claim under GINA, the plaintiff would have needed to allege that his employer used his wife's diagnosis "to forecast the tendency of any other individual to contract multiple sclerosis." Poore at 731.

Similarly, a diagnosis of HIV is not genetic information protected by GINA. In a North Carolina case, a plaintiff claimed that his employer wrongfully disclosed confidential information about the plaintiff's HIV status to coworkers and customers in violation of GINA. The court stated that "Neither Plaintiff's HIV diagnosis, kidney failure, nor viral gastroenteritis constitute genetic information about a manifested disease or disorder [and] an HIV test is not an example of a genetic test." Hoffman v. Family Dollar Stores, Inc., 99 F. Supp. 3d 631, 637 (referencing Background Information for EEOC Final Rule on Title II of GINA, *available at* http://www.eeoc.gov/laws/regulations/gina-background.cfm).

What employers must comply with GINA?

A GINA-covered entity is an employer, employing office, employment agency, labor organization or joint labor-management committee with at least 15 employees for each working day in each of 20+ calendar weeks in the current or preceding calendar year. (29 CFR 1635.2(c)(1)). A covered entity's actions must apply to its workforce in their capacity as employees, members of a labor organization, or a participant in an apprentice program. This means that GINA would not apply to a hospital employee undergoing a medical examination at its employer's facility for reasons unrelated to employment. GINA also would not apply to law enforcement employers investigating criminal conduct.

When can my employer know my genetic information?

The most common reasons for an employer to know of an employee's genetic information are somewhat predictable. Even in these situations, the employer cannot use any genetic information to discriminate against an employee.

- Inadvertent knowledge: If an employer learns about an employee's genetic information accidentally or overhears a conversation about a sick child or a test result, there is a GINA violation.
- Public information: If an employer learns about genetic information through the newspaper or other publicly available resources, the employer has not violated GINA.

- Family and Medical Leave Act (FMLA): If an employee needs to take time away from work to care for a sick family member, questions and forms required to approve such leave may ask about genetic information if pertinent.
- Voluntary health services: Employers can offer voluntary health or genetic services, including wellness programs. If these programs are truly voluntary, then forms, questionnaires, and health care providers overseeing the programs may ask for health histories, including genetic information.

Until recently, employers were permitted to offer employees an inducement to provide his or her current health status information as part of a health risk assessment administered in connection with an employee-sponsored wellness program. As outlined above, GINA allows employers to ask health-related questions and to conduct medical examinations if doing so is voluntary for employees. In 2017, AARP challenged the "voluntary" nature of employee wellness program financial incentives, arguing that such incentives (up to 30% of the cost of health insurance coverage) was coercive. Ultimately, the DC District Court, while affording Chevron deference, determined that EEOC failed to make a case that 30% incentives satisfy the "voluntary" requirement under GINA, and the Court remanded the matter to EEOC to revise its rules (See AARP v. EEOC, 292 F. Supp. 3d 238 (DDC 2017), *available at* https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2016cv2113-47). In December 2018, EEOC published a final rule removing the provision that allowed employers to offer financial incentives to employees that participate in wellness programs. (83 Fed. Reg. 65296 (Dec. 20, 2018)). Employers may still ask employees about genetic information as part of employee wellness programs; however, the provision of information must be voluntary, meaning the employer neither requires the individual to provide such information nor penalizes those who choose not to provide it. (29 CFR § 1635.8(b)(2)(i)(B)).

What can lawyers do to protect employers from inadvertent disclosures of genetic information?

The Title II regulations provide sample language that covered employers may want to include in any contract that may result in disclosures of medical information. With this language, any receipt of genetic information along with medical information will be deemed inadvertent:

> *The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA Title II from requesting or requiring genetic information of an individual or family member of the individual, except as specifically allowed by this law. To comply with this law, we are asking that you not provide any genetic information when responding to this request for medical information. 'Genetic information' as defined by GINA, includes an individual's family medical history, the results of an individual's or family member's genetic tests, the fact that an individual or an individual's family member sought or received genetic services, and genetic information of a fetus carried by an individual or an individual's family member or an embryo lawfully held by an individual or family member receiving assistive reproductive services.*

See 29 CFR § 1635.8(b)(1)(B).

III. Confidentiality of Alcohol and Drug Abuse Patient Records[3]

The privacy provisions in 42 CFR Part 2 were motivated by the understanding that stigma and fear of prosecution might dissuade persons with substance use disorders from seeking treatment. To add an extra layer of protection on these records, the regulations outline under what limited circumstances information about a patient's treatment may be disclosed with and without the patient's consent.

The Substance Abuse and Mental Health Services Administration (SAMHSA) released a final rule (the "Final Rule") in January 2017 modernizing the confidentiality requirements for substance use disorder (SUD) patient records (also known as 42 CFR Part 2, or "Part 2"). Twelve takeaways from the Final Rule and subsequent SAMHSA guidance are as follows:

1) SAMHSA has clarified the definition of "Part 2 Program."

The confidentiality requirements of Part 2 apply to Part 2 Programs, which generally include SUD programs (a) conducted, licensed, or funded by a federal department or agency; or (b) that are tax exempt or receive tax deductions for contributions ((a) and (b) are collectively referred to as "Federal Support"), and (c) which hold themselves out as providing and actually do provide SUD diagnosis, treatment, or referral for treatment. SAMHSA has clarified that a Part 2 Program can be (i) an individual or entity; (ii) an identified unit within a general medical facility (e.g., hospital, trauma center, or federally qualified health center); or (iii) medical personnel or staff within a general medical facility whose primary function is SUD diagnosis, treatment or referral. In each instance, the Program must receive Federal Support and hold itself out and actually provide SUD services.

2) SAMHSA recognizes the growing list of mind-altering substances.

Previously, Part 2 applied to disclosures that "would identify a patient as an alcohol or drug abuser." Now, Part 2 applies to SUDs, which are defined as "a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired, control, social impairment, risky use, and pharmacological tolerance and withdrawal." The definition does not include tobacco or caffeine use. In commentary, SAMHSA provides examples such as alcohol, cannabis, hallucinogens, inhalants, opioids, sedatives, hypnotics, anxiolytics, and stimulants.

3) A "Treating Provider Relationship" may exist prospectively.

To better illustrate the consent requirements (described in numbers 4-6 below), SAMHSA defined a "treating provider relationship" to include the traditional, voluntary physician-patient relationship where an in-person visit has already occurred. However, recognizing that some SUD patients are involuntarily confined, it expanded the definition to include situations where (i) the patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated or agrees to accept consultation for a SUD condition; and (ii) the individual or entity undertakes or agrees to

[3] Material in this section is taken in part from Breuer, JR and Fosheim, GE, *Top 10 Takeaways from SAMHSA's Recent Update of Substance Use Disorder Confidentiality Regulations*, 3 PRATT'S PRIVACY & CYBER SECURITY L. REPORT 185 (2017); and Breuer, JR and Fosheim, GE, *SAMHSA Continues to Refine Part Two Regulations* (available at https://www.drinkerbiddle.com/insights/publications/2018/01/samhsa-continues-to-refine-part-two-regulations).

undertake diagnosis, evaluation, or treatment of or consultation with the patient for any SUD condition. As a result, Part 2 obligations may arise for providers even before an initial patient encounter occurs.

4) Broad consent is permissible for disclosures of Part 2 Program information to others with Treating Provider Relationships.

A Part 2 Program must obtain patient consent to disclose Part 2 Program information to an entity with which the patient has a Treating Provider Relationship. The consent must be in writing (paper or electronic) and include:

(i) The patient's name;

(ii) The Part 2 Program permitted to make the disclosure;

(iii) The amount and kind of SUD-related information to be disclosed; and

(iv) The name of the individual or entity that is to receive that information.

A sample patient consent is available at Appendix B. Patients may also give broad consent for disclosure to classes of individuals or entities who may have future Treating Provider Relationships, even though their identity is not known at the time of consent. In this case, the consent must include a general description of the individual or entity, or class of individuals or entities to whom disclosure may be made. The consent must also inform the SUD patient of his or her rights to request and receive a list of individuals and entities to which their Part 2 Program information has been disclosed pursuant to a general description.

Tracking disclosures may prove to be burdensome to Part 2 Programs. Part 2 Programs are not allowed to use a broad or general consent until they have a methodology in place to track the disclosures necessary for a patient accounting.

5) Specific consent is required for Part 2 Program disclosures outside of a Treating Provider Relationship.

For a Part 2 Program to disclose SUD-related information to a third party outside of Treating Provider Relationship, the consent must contain each of the elements described in 4(i) through 4(iv) above. Each must be described with specificity and by name.

6) Disclosure without consent is permissible only in very limited circumstances.

SAMHSA outlined three circumstances in which patient consent is not required to disclose SUD-related records: (1) Bona fide medical emergencies; (2) Research; or (3) Audits.

Part 2 Programs may disclose SUD-related records to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient's consent cannot be obtained. In a medical emergency, the Program must immediately document, in writing: (i) the name of the recipient and their affiliation with a health care facility; (ii) the name of the disclosing party; (iii) the date and time of the disclosure; and (iv) the nature of the emergency. SAMHSA clarified that legal incapacity to consent may qualify in an involuntary commitment situation; however, if the patient refuses to consent and has legal capacity to do so, the situation cannot be deemed one in

which consent cannot be obtained. SAMHSA plans to release additional guidance regarding medical emergencies that would be valid grounds to release SUD-related records.

Part 2 Programs may also disclose SUD information for the purpose of conducting scientific research if person with responsibility for disclosure determines that (i) the recipient is a covered entity or business associate under HIPAA and has obtained appropriate authorization or waiver from the patient; (ii) the recipient is subject to the human subjects protection Common Rule (45 CFR Part 46) and has obtained the patient's informed consent or an appropriate waiver or exemption; or (iii) both HIPAA and Common Rule compliance is met, when applicable. Researchers must not re-disclose patient information, may include data in research reports only in a non-identifiable aggregate form, must follow Part 2 storage requirements including destruction of SUD-data, and must retain the patient records in accordance with all applicable laws.

Finally, Part 2 Programs may disclose SUD information without patients' consent for audit or evaluation purposes. The Part 2 Program must determine that the recipient is qualified to audit the Program. Permitted auditors may include entities reviewing Part 2 Programs on behalf of Medicare, Medicaid, CHIP, or federally regulated accountable care organizations. The regulations regarding audit disclosures without consent are extremely complex. Part 2 Programs are encouraged to review the regulations carefully and consult with legal counsel.

7) **Part 2 Programs must have policies and procedures to prevent unauthorized users and disclosures of Program information.**

The Final Rule requires Part 2 Programs and lawful holders of Part 2 Program information to have formal policies and procedures in place to protect against unauthorized uses and reasonably anticipated threats or hazards to patients' identifying information. The policies and procedures must address (i) transferring, removing, destroying, and maintaining paper records; (ii) physical safeguards for paper records at workstations and cabinets; (iii) rendering patient identifying information in paper records non-identifiable or with a low risk of re-identification; (iv) creating, receiving, maintaining and transmitting electronic records; (v) destroying electronic medical records and sanitizing storage media; (vi) using and accessing electronic medical records; and (vii) rendering patient identifying information in electronic records non-identifiable or with a low risk of re-identification. Notably, courts, law firms, family members and private citizens are not considered "lawful holders" for disclosure purposes and thus are not required to prepare policies and procedures.

8) **Part 2 may look, talk and smell like HIPAA, but it is not HIPAA.**

Many commenters suggested aligning Part 2 confidentiality requirements with HIPAA, proposing that Part 2 Program information be treated like psychotherapy notes under HIPAA. SAMHSA noted its attempts at such alignment in the Final Rule, but repeatedly reminded commenters that Part 2 provides more stringent federal protections than are required under other health privacy laws. This suggests that providers risk non-compliance by relying solely on their HIPAA policies to safeguard Part 2 Program patients' privacy.

9) **Part 2 Programs must inform patients of their confidentiality rights and may not confirm or deny patient status.**

When patients are admitted to Part 2 Programs or as soon as practicable thereafter, that patient must receive paper or electronic notice of their rights under Part 2 Programs. The notice must include contact information and appropriate authorities for reporting Part 2 violations. In addition, Part 2 Programs are prohibited from issuing statements such as "an identified individual is not and has never been a patient." One commenter illustrated how such statements could give rise to third-party expeditions when the Program answers with silence. Previously, the regulations did not restrict such a disclosure.

10) SAMHSA has promulgated subsequent rulemaking since the Final Rule.

In a final rule published on January 3, 2018, SAMHSA took further steps to modernize Part 2 and to align the regulations with the way health care is delivered in the United States. Specifically, SAMHSA:

1. Provided an option for an abbreviated redisclosure prohibition notice in recognition of electronic medical record (EMR) character limitations.
2. Established that lawful holders of Part 2 data may disclose such data to contractors, subcontractors and legal representatives for payment and health care operations-related purposes without specific consent.
3. Clarified that government entities funding Part 2 programs may have access to program information as necessary to conduct audits and evaluations without patient consent, and similarly may share Part 2 information with contractors, subcontractors and legal representatives for audit and evaluation purposes.

42 CFR § 2.32 requires disclosures made with SUD patients' consent to include a lengthy written statement informing the recipient that the information may not be further disclosed without specific patient's consent or as otherwise permitted by law. SAMHSA sought comments on whether an abbreviated notice should be permissible and, if so, the circumstances in which such notice might be appropriate.

After acknowledging that many EMR systems have internal codes, flags, pop-ups and other signifiers in place to protect health information under HIPAA and other privacy laws, SAMHSA discussed that an abbreviated notice may be useful primarily in EMRs with character-limited free-text fields (often 80 characters or fewer). In the final rule, however, SAMHSA declined to limit use of an abbreviated notice to EMR free-text fields. Instead, SAMHSA amended 42 CFR § 2.32 to allow lawful holders of Part 2 information to append the following redisclosure notice any time notice is required under the Part 2 regulations:

> "42 CFR part 2 prohibits unauthorized disclosure of these records."

Lawful users also may continue to use the longer redisclosure prohibition language found at 42 CFR § 2.32(a)(1). This language is provided in Appendix C.

11) Authorized Disclosures for Payment and Health Care Operations Purposes

42 CFR § 2.33 allows a Part 2 program to disclose SUD patient records upon obtaining the patient's written consent to any person identified in the consent. SAMHSA proposed to permit disclosure of such information to contractors, subcontractors and legal representatives without patient consent for specifically identified payment and health care operations activities. In so doing, SAMHSA recognized the practical importance of allowing such disclosures rather than requiring Part 2 programs

to list each contractor, subcontractor or legal representative on a consent form or to obtain new consents whenever a contractor is changed.

Although the final rule does not include the list of approved payment and operations activities in the regulations, SAMHSA includes in the preamble to the final rule the activities listed in Table 1 below as non-exclusive examples of payment and health care operations for which disclosure without patient consent is permissible. Importantly, unlike HIPAA, "health care operations" under Part 2 do not include care coordination and case management activities. Nor does the final rule permit Part 2 programs to disclose Part 2 information to contractors, subcontractors and legal representatives for treatment, diagnosis or referral purposes. SAMHSA emphasized the importance of patient choice in disclosing information protected by Part 2 to health care providers with whom patients have direct contact.

Part 2 programs that wish to disclose Part 2 information to contractors, subcontractors or legal representatives for payment and health care operations purposes are required to have agreements in place with such third parties. The agreements must include provisions requiring compliance with Part 2 and must make clear that the contractor, subcontractor or legal representative is fully bound by the provisions of Part 2 and that unauthorized redisclosure is prohibited. Common contract language obligating "compliance with all applicable federal and state laws" will not suffice. We recommend that Part 2 programs include language similar to the following when entering into agreements with contractors, subcontractors and legal representatives to provide payment and/or health care operations support:

> *"[Contractor] hereby acknowledges that it is fully bound by the provisions of 42 CFR Part 2 upon the receipt of any Part 2 program patient identifying information. 42 CFR Part 2 prohibits unauthorized disclosure of these records. [Contractor] shall implement all reasonable and appropriate safeguards to prevent unauthorized uses and disclosures of Part 2 program information and shall report any unauthorized uses, disclosures, or breaches of patient identifying information to [Lawful Holder]."*

Part 2 programs should ensure that any Part 2 program information disclosed is consistent with the purposes set forth in the patient's consent and is comprised of only the minimal information necessary to meet the payment or health care operations need. Part 2 programs must incorporate the required language into their contracts by February 2, 2020.

Table 1. Non-exclusive Examples of Payment and Health Care Operations

- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, claims filing, and related health care data processing.
- Clinical professional support services (e.g., quality assessment; utilization management).
- Patient safety activities.
- Activities pertaining to (i) training of students and health care professionals; (ii) assessing practitioner competencies; (iii) assessing provider or health plan performance; or (iv) training of non-health care professionals.
- Accreditation, certification, licensing or credentialing activities.
- Underwriting, enrollment, premium rating and other activities relating to health insurance or health benefit contracts, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care.
- Third-party liability coverage.
- Activities related to fraud, waste and abuse.
- Conducting and arranging for medical review, legal services and auditing functions.
- Business planning and development, such as cost management and planning-related analyses, including formulary development and administration and developing or improving methods of payment or coverage policies.
- Business management and general administrative activities.
- Customer services, including providing data analyses for policy holders, plan sponsors and other customers.
- Resolution of internal grievances.
- Transactional needs, including sale, merger, consolidation or dissolution of an organization.
- Determinations of eligibility for coverage and adjudication or subrogation of health benefit claims.
- Risk adjusting amounts due based on enrollee health status and demographic characteristics.
- Review of health care services for medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.

12) Disclosures for the Purpose of Audits and Evaluations

Many Part 2 programs receive financial support from federal, state or local governments. SAMHSA recognizes the need for such governmental entities to audit and evaluate the Part 2 programs for compliance with applicable laws, rules, regulations and policies. SAMHSA also recognizes the practical need for such governmental entities to hire contractors, subcontractors and legal representatives to conduct audits and evaluations on their behalf.

In the final rule, SAMHSA clarifies that federal, state and local governmental entities may receive Part 2-protected patient identifying information directly from the lawful holder when auditing or evaluating a Part 2 program. Patient consent is not required for this purpose or for further redisclosure by the governmental entity to a contractor, subcontractor or legal representative to conduct the audit or evaluation. As with any disclosures, Part 2 programs should limit the information to the minimum necessary to accomplish the task.

IV. California Consumer Privacy Act of 2018

On June 28, 2018 California passed this law which takes effect on 1/1/2020. It is one of the strictest privacy laws in the country, and has parallels to the EU's GDPR. In effect, the Act grants consumers a right to request a business to disclose the categories and specific pieces of information that it collects about the consumer, where it gets personal information, the business purpose for collecting or selling personal information, and with whom that information is shared.

Regulations are forthcoming by the California Attorney General who is tasked with enforcing compliance. Specific details of the Act are as follows:

- Personal information includes information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
- Examples include:
    - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
    - Characteristics of protected classifications under California or federal law;
    - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
    - Biometric information;
    - Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Website, application, or advertisement;
    - Geolocation data;
    - Audio, electronic, visual, thermal, olfactory, or similar information;
    - Professional or employment-related information;
    - Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act;
    - Inferences drawn from any of the information above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Companies must post a privacy notice that:
    - lists the categories of personal information collected,
    - sources of personal information,
    - purposes for collecting,
    - categories of third parties it is shared with, and lists the categories of personal information sold/shared with others for a business purpose or a representation that it has not done so.

- Companies must respond to customer requests for information about the personal information that has been collected by detailing:
    - the categories of all personal information that have been collected online or offline;
    - the sources from which the information was collected;
    - the business purposes for collecting;
    - the categories of third parties that info is shared with (including vendors and service providers); and
    - the specific pieces of personal information collected about the customer.
- Customer requests for this information must be accepted online and by phone and the customer must be responded to through a customer's "account", or if they do not have an account, by mail or electronically at customer's option. Electronically formatted responses must be in a "readily useable format" so the data can be transferred to another entity.
- Customers have right to request deletion of any personal information that has been collected, with only narrow exceptions. When responding to a customer deletion request, the company must direct vendors to delete any personal information from their records.
- If company sells or shares personal information (including with vendors or service providers for business purposes) it must:
    - Respond to customer requests with details about personal information sold/shared, and categories of third parties sold to/shared with
    - Offer customers the ability to opt-out of sales of personal info (n/a to sharing for business purpose)
    - If information is sold, companies must have a "do not sell my information" link on their homepage and a publicly available webpage providing details about selling information and opting out.

V. Cyber Security Tips and Considerations

1) Data Security Generally

a. Also called Information Security or Cybersecurity
    i. As opposed to physical security, which is also important, but which is well understood

b. Data security is of the utmost importance, whether or not you access, store or process regulated data (PHI, PII).
    i. For lawyers & organizations, Data Security must be baked in to everything, especially if you're dealing with regulated data like Patient Health Information.

c. "Data Security is a journey, not a destination."
    i. It's not about installing one security product or doing a security audit or assessment every so often. Those things can help, but they may not be enough.
    ii. It helps to install the right software tools that help maintain data security, but also important to use them the right way with consistent processes.

2) Organizational Data Security

a. If you're big enough to employ IT professionals,
    i. Best to have staff dedicated to data security. A Chief Information Security Office (CISO), if possible.
    ii. Whether dedicated or not, your IT team should keep up with evolving

security best practices, and it should be a major component of their job.

b. If you're not big enough to have an IT department,
    i. You have to rely on vendors to keep you secure.
    ii. Well known vendors are more likely to have high quality data security practices.
c. It's helpful/required to have consistent policies & procedures, about which employees are educated.
d. It's helpful/required to have an Incident Response Plan that includes potential for Cyber-related incidents
    i. E.g., do you know how to react if/when you have a breach of regulated data?
    ii. See Attachment D for a sample letter notifying individuals of a breach of their personal information.
e. It's helpful/required to have an inventory of all systems & locations where regulated data may be stored or processed.
    i. Sometimes called "Data Maps"
    ii. Enables a systematic process for evaluating security of regulated data throughout your organization.
    iii. Include systems whether regulated data is "in transit" (email) or "at rest" (databases, hard drives)
f. It's helpful/required to perform regular/annual data security risk assessments
    i. Use your data maps to review the data security and related processes.
    ii. If/when you find shortcomings, make a plan to remediate the problems.

3) Vendor Data Security

a. You are more than likely relying on some kind of third party to store or process sensitive data.
    i. Gmail, Google Docs, Office 365 all use the Internet or "the Cloud"
    ii. Well-known cloud and Software-as-a-Service (SaaS) vendors are more likely to use the latest best practices for data security.
    iii. Less well-known cloud and SaaS vendors should be investigated for security practices.
        1. *Do they have a SOC 2 report for their data center?*
        2. *For HIPAA, will they sign a Business Associate Agreement (BAA)?*
b. For regulated data, use vendors who explicitly state they are secure.
    i. For example, "HIPAA Compliant Security" or "HITRUST Certified"
        1. *No specific certification authorized under HIPAA, but HITRUST is an industry-driven certification that comes close.*
    ii. Be prepared to potentially audit your vendors' security practices.

4) Personal Data Security

a. Regardless of size or type of organization, we all need to be responsible for our own personal data security
b. Two-Factor Authentication
    i. Use two-factor authentication wherever it's offered.
    ii. In general, logging in always requires you to provide:
        1. *something you know (like a password or a pin code),*

2. *something you are (your face, your fingerprint), or*
3. *something you have (your phone, a key).*

iii. Two factor (or sometimes called multi-factor) requires that you provide something from at least two of these categories, like a code texted to your phone, in addition to your account password.

iv. Especially for accounts & websites that access regulated data (PHI or PII), financial (a bank), or are closely tied to your identity or your organization's identity (e.g., Facebook, Google, Twitter, LinkedIn)

v. Using a code from an authenticator app (e.g., Google Authenticator) or a hardware authenticator is better than a code texted to your phone, but any two-factor is better than no two-factor

c. Passwords & Password Managers

i. Don't reuse passwords and use a password manager

ii. Reusing passwords makes it easy for hackers to break into other sites if they happen to get access to one site's passwords, which happens far too often.

iii. A reputable Password Manager (e.g., LastPass, 1Password) installs on all your devices, syncs across those devices, and acts as a secure storage locker for all your passwords, so you don't have to remember them all, just the main password for your password manager.

iv. A Password Manager can also generate different complex passwords for each account, and since you use the Password Manager to retrieve them each time you log in, you don't have to remember them.

d. Hard Drive Encryption

i. Encrypt your hard drive

1. *Turn on BitLocker on Windows machines*
2. *Turn on FileVault on Mac machines*

ii. Encrypting your hard drive makes it virtually impossible for someone to access your files in the situation where your computer is lost or stolen.

Appendix A

Sample Business Associate Agreement[4] (available at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html**)**

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured

[4] Although this language is made available by the Department of Health and Human Services, we strongly recommend consulting with experienced health care counsel before entering into a business associate agreement.

protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate

obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and

5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Appendix B

CONSENT FOR THE RELEASE OF CONFIDENTIAL SUBSTANCE USE DISORDER TREATMENT INFORMATION

Instructions: *Please read this consent form it its entirety before proceeding. Your consent allows _____ to release your substance use disorder treatment information to individual(s) or organization(s) you specifically name. Please provide the requested information on the spaces below.* **The form must be signed and dated for authorization.**

Name: _____

I authorize _____ *(insert name or general designation of individual or program)* **to release the following information** *(check all that apply)***:**

From dates: _____ to _____: ☐ **All my substance use disorder treatment information**; ☐ **Medication(s) only**; ☐ **Physician's Order(s)**; ☐ **Progress Notes**; ☐ **Laboratory/Diagnostic Studies**; ☐ **Plan(s) of Care;** ☐ **Discharge Summary(ies);** ☐ **Other** *(please specify)***:** _____
_____

to the following individual(s) or organization(s) *(attach a separate sheet if necessary)***:**

☐ **Individual** *(E.g., Treating provider or any specifically named individual, e.g. spouse, parent, child)***:**
_____
_____

☐ **Organization/Facility with which Patient has a Treating Provider Relationship** *(Name of Org.)***:**_____
_____

☐ **Insurance Provider** *(Name of Payor)***:**
_____

☐ **Research Institution** *(Name of Institution)***:**
_____ **AND**
☐ Name(s) of individual(s) at Institution:_____ **OR**
☐ Name(s) of organization(s) with a treating provider relationship:_____
_____**OR**
☐ To all my treating providers who participate in the Institution, past, present and future
☐ If you elect to disclose information to all your treating providers, past and present, you have the right to request that _____ provide you with a list of entities to which your information has been disclosed for the last two years. *(If you elect this designation, please check the box to the left confirming that you understand that you may ask for this list of disclosures at any time.)*

***For further disclosure to*:**
☐ Name(s) of individual(s): _____ **OR**
☐ Name(s) of organization(s) with a treating provider relationship:_____**OR**
☐ To all my treating providers, past, present and future
☐ If you elect to disclose information to all your treating providers, past and present, you have the right to request that _____ give you a list of entities to which your information has been disclosed for the last two years. *(If you elect this designation, please check the box to the left confirming that you understand that you may ask for this list of disclosures at any time.)*

For the limited purpose of *(circle any or insert purpose)***:**

- ☐ **Treatment**
- ☐ **Care coordination**
- ☐ **For billing purposes**
- ☐ **To provide an update about my status to specifically named individual(s)/organization(s) listed above**
- ☐ **Other reason(s):_____**
  _____

I also understand that I may revoke this consent at any time (verbally or in writing) except to the extent that any action was taken in reliance on it.

If not previously revoked, this consent will expire on/when/if (add date or event): _____
_____ **OR**
one year from today's date, whichever is earlier.

Signature *(or individual authorized to give consent and sign)*:

_____

Date:

_____

I understand that any records relating to treatment of a substance use disorder are protected under federal regulations governing Confidentiality of Substance Use Disorder Patient Records, 42 C.F.R Part 2, and 45 C.F.R Parts 160 and 164, as well as **[insert applicable State laws]** and cannot be disclosed without my written consent unless otherwise provided for in the law.

Appendix C

NOTICE TO PARTY RECEIVING SUBSTANCE USE DISORDER INFORMATION

This information has been disclosed to you from records protected by Federal confidentiality rules (42 C.F.R Part 2). The Federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 C.F.R Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at 42 C.F.R §2.12(c)(5) and §2.65.

Appendix D

Breach Notification Letter

[DATE]

Important Security and Protection Notification. Please read this entire letter.

Dear _____

[WE] recently learned that the security of certain of our information systems was compromised by a criminal cyber attack apparently designed to collect Social Security numbers, credit card numbers and other financial information. Between **[DATE RANGE]** our forensic investigators confirmed that this attack potentially exposed certain of your information to unauthorized access and acquisition. I say "potentially" because, to date, there is no evidence that any information was actually accessed or acquired as a result of this criminal invasion. However, the information potentially exposed may have included your name, contact information, medical or healthcare information, date of birth, credit card information, Social Security number and health insurance account number. Based upon our investigation, the period during which your information may have been exposed appears to have been between **[DATE RANGE]**.

Out of an abundance of caution, we want to make you aware of the attack and our efforts to help safeguard your information. Immediately upon learning of this criminal attack and the potential exposure of private patient information, **[WE]** took action. Specifically, upon learning of the potential of this incident, we promptly took the following actions: (i) curtailed the intrusion; (ii) hired numerous experts, including two leading national forensic investigation firms, to help us investigate the situation and determine the individuals and information potentially affected; and (iii) began the process of notifying potentially affected individuals. In addition, we have notified law enforcement and are taking steps to further guard against this type of criminal attack in the future.

As always, we recommend that you remain vigilant by reviewing your explanation of benefits for medical services and financial account statements, as well as free credit reports for unauthorized activity. From the moment we learned of the potential exposure, our primary concern has been ensuring that you are protected against risks related to this incident. Therefore, we have engaged _____, one of the leading providers of credit monitoring products, to provide you with its _____, including credit monitoring, for one year at no cost to you. Enclosed with this letter is information regarding these services and instructions for enrollment, as well as an insert providing additional useful information regarding steps you can take to protect yourself against identity theft. We have also engaged _____ to provide a dedicated call center to answer questions about this incident. If you have any questions regarding this incident or would like assistance enrolling in _____, please contact _____.

We take your privacy very seriously. We sincerely regret that this unfortunate attack occurred and we apologize for any inconvenience or concern it may cause you. We value our relationship with you and remain committed to serving the needs of our community.