Managing Payment Compliance

Michelle Tygart, ClearBalance Healthcare

Disclaimer

This presentation is designed to provide general information on pertinent legal topics. The information is provided for educational purposes only. Statements made or information included do not constitute legal or financial advice.

Compliance Issues

- Data Security
  - PCI DSS standards imposed by credit and debit card processors and banks
  - Data breach notification laws
  - Red Flags Rule
  - HIPAA
  - Identity Theft
- Federal and State laws applicable to payment plans
- Extraordinary Collection Actions
- Cash payments over $10,000
- Regulation E
- NACHA
- Debt Collection Practices

PCI DSS

- Mandatory compliance program resulting from a collaboration between the credit card associations to create common industry security requirements for cardholder data.
- Common set of industry tools and measurements to ensure safe handling of sensitive information.
- Actionable framework for developing a robust account data security process—including preventing, detecting, and reacting to security incidents.
- Technical requirements for secure storage, processing, and transmission of cardholder data.
- Common auditing and scanning procedures.

PCI DSS

- If you ***store, access, transmit, or process*** cardholder data, you must comply with the Payment Card Industry Data Security Standard ("PCI DSS")

- Applies to credit card business transacted over all business channels (point of sale (POS), mail, e-commerce, interactive voice response (IVR))

- Penalties for non-compliance include:
  - Fines from the Card Associations via your payment processor;
  - Damages claims from patients, guarantors and other payors; and
  - Fines from the State.

- PCI DSS compliance must be certified each year:
  - Can be compliant yourself - cost hundreds of thousands of dollars; or
  - Can use payment processor that is compliant and avoid ever receiving access to cardholder data.

Data Breach Notification Laws

- The HHS HIPAA Breach Notification Rule requires providers and their business associates to provide notification to affected persons (and in some cases to prominent local media outlets and the HHS Secretary) following an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of unsecured protected health information (PHI)
- Vendors of personal health records and their third party service providers are subject to similar breach notification provisions under a rule administered by the Federal Trade Commission.

Data Breach Notification Laws

- All 50 states have enacted security breach laws that require, among other things:
  - Encryption and protection of PII;
  - Immediate investigation of any suspected data breach; and
  - Prompt notification to affected persons (and in some cases state attorney general and law enforcement) of data breaches involving personal information.
  - Texas data breach notification law requires providers to notify individuals and the Texas Attorney General after discovering or receiving notification of "any breach of system security." The notice must go to any individual whose sensitive personal information was, or is reasonably believed to have been, breached within 60 days. The Texas Attorney General must be notified within 60 days if the breach involves at least 250 Texas residents. In 2021 the rule was amended to require a more detailed response of what has occurred and a public listing of breaches.

Data Breach Notification Laws

- Penalties for non-compliance can include:
  - Damages to each consumer (typically minimum of $1,000 per consumer, some states are higher); and
  - Fines from the state (e.g., Florida increases damages every day that lapses since discovery date up to $500,000).
- Requirement to notify State AG and law enforcement leading to scrutiny of all practices.

Identity Theft

- A provider's staff should be alert for the possibility of identity theft, including but not limited to these circumstances:
  - A complaint or question from a patient based on the patient's receipt of:
    - A bill for another individual;
    - A bill for a product or service that the patient denies receiving;
    - A bill from a healthcare provider that the patient never patronized; or
    - A notice of insurance benefits (or explanation of benefits) for healthcare services never received.
  - A dispute of a bill by a patient who claims to be the victim of any type of identity theft
  - A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance
  - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient
  - The patient submits a driver's license, insurance card or other identifying information that appears to be altered or forged
  - The Social Security number or other identifying information the patient provided is the same as identifying information in the provider's records provided by another individual, or the Social Security number is invalid.

FTC Red Flags Rule

- Applies to providers who regularly enter into payment plans with obligors to defer the payment for services
- Providers must develop and implement an Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft (fraud committed or attempted using the identifying information of another person without authority) in connection with a payment plan.
- Program must be appropriate for the size and complexity of the provider and the nature and scope of its activities.

FTC Red Flags Rule

- An Identity Theft Prevention Program must include reasonable policies and procedures to:
  - Identify relevant patterns, practices or specific activities that indicate the possible existence of identity theft (Red Flags) for payment plans, and incorporate those Red Flags into the program;
  - Detect Red Flags that have been incorporated into the provider's Program;
  - Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
  - Ensure the Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the provider from identity theft.

FTC Red Flags Rule

- Administration of Identity Theft Prevention Program:
  - Provider must obtain approval of the initial written Program from either its board of directors or an appropriate board committee;
  - Must involve the board (or appropriate board committee) or a designated senior manager in oversight, development, implementation and administration of the Program;
  - Must train staff, as necessary to effectively implement the Program; and
  - Must exercise appropriate and effective oversight of service provider arrangements.

HIPAA Privacy Rule

- Regulation issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA)
- Establishes national standards to protect an individual's medical records and other individually identifiable health information (collectively defined as protected health information (PHI)) and applies to health care providers that conduct certain health care transactions electronically.
  - Can include medical billing records
- Requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made without an individual's authorization.
- Gives individuals rights over their PHI, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

HIPAA Security Rule

- Ensures the confidentiality, integrity, and availability of PHI created, received, maintained, or transmitted electronically
- Protects against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protects against any reasonably anticipated uses or disclosures of such information that are not permitted

HIPAA Breach Notification Rule

- Requires covered entities to notify individuals when their unsecured PHI is impermissibly used or disclosed – or “breached” – in a way that compromises the privacy and security of the PHI

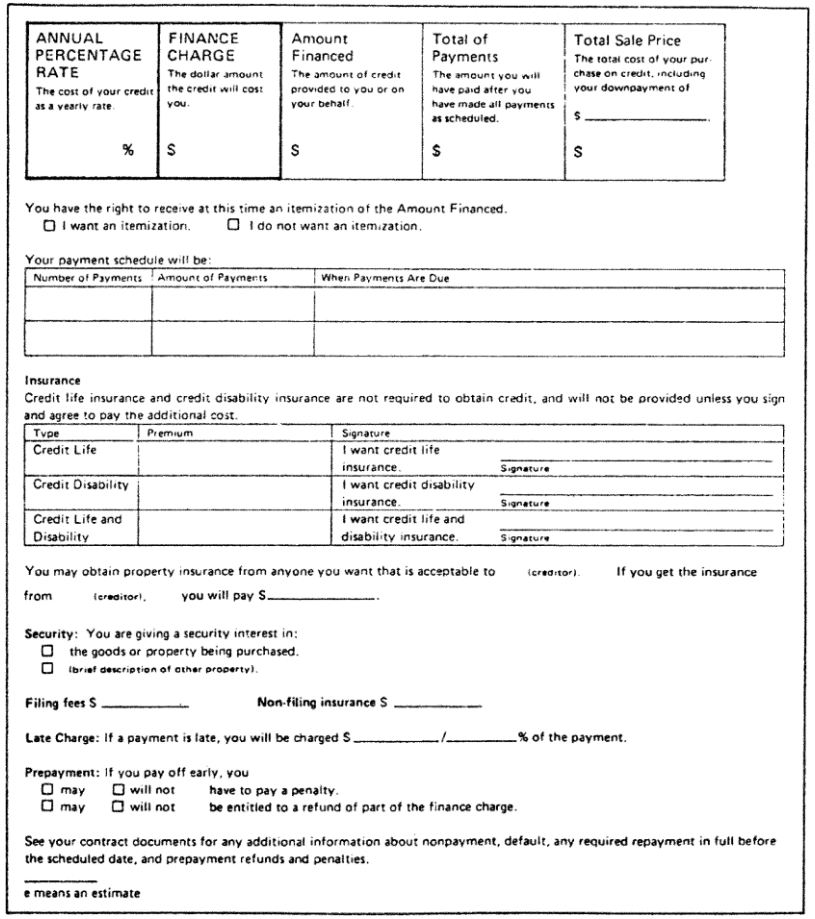
Breach of Unsecured PHI

- Unsecured PHI is PHI that is “not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified” by HHS in guidance. Covered entities that take the steps to secure PHI as specified in this guidance will not be required to provide notification in the event of a breach.
- A breach is an “unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information.”
- Upon discovery of a breach of unsecured PHI, the covered entity must determine (and document) if there is a “low probability” that the PHI has been compromised by completing a risk assessment. The risk assessment must take into account at least the following four factors:
  - nature and extent of PHI involved, including types of identifiers, the likelihood of re-identification and the sensitive nature of the information;
  - who used the PHI or to whom was the PHI disclosed, including whether the unauthorized person has an obligation to protect the privacy and security of the information or has the ability to re-identify the information;
  - whether the PHI was actually acquired or viewed; and
  - extent to which the risk to the PHI has been mitigated.
- Upon a breach of unsecured PHI, covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the breach. Must also notify Secretary of HHS and in some cases the media.

Truth in Lending Act Disclosures for Payment Plans

- When a provider enters into a payment plan which either (i) charges interest or a finance charge or (ii) is payable in more than four installments (not including a downpayment made on the date of the agreement), the provider must comply with the federal Truth in Lending Act and CFPB Regulation Z (TILA)
  - Requires very particular disclosures and format; consult with an experienced attorney familiar with TILA
  - Restrictions on advertising of payment plans
  - Significant civil and possibly criminal liability for failure to comply
    - In a class action, a court may award damages of up to $1 million or 1% of the provider's net worth, in addition to actual damages, legal fees and costs
  - Exception: If the amount owing (after any downpayment) exceeds the threshold amount set by the CFPB in effect on the date of the agreement ($69,500 for agreements entered into in 2024).

Truth in Lending Act Disclosures for Payment Plans



ANNUAL PERCENTAGE RATE The cost of your credit as a yearly rate. %	FINANCE CHARGE The dollar amount the credit will cost you. $	Amount Financed The amount of credit provided to you or on your behalf. $	Total of Payments The amount you will have paid after you have made all payments as scheduled. $	Total Sale Price The total cost of your purchase on credit, including your downpayment of $ _____. $

You have the right to receive at this time an itemization of the Amount Financed.
☐ I want an itemization. ☐ I do not want an itemization.

Your payment schedule will be:

Number of Payments	Amount of Payments	When Payments Are Due

Insurance
Credit life insurance and credit disability insurance are not required to obtain credit, and will not be provided unless you sign and agree to pay the additional cost.

Type	Premium	Signature
Credit Life		I want credit life insurance. _____ Signature
Credit Disability		I want credit disability insurance. _____ Signature
Credit Life and Disability		I want credit life and disability insurance. _____ Signature

You may obtain property insurance from anyone you want that is acceptable to (creditor). If you get the insurance from (creditor), you will pay $_____.

Security: You are giving a security interest in:
☐ the goods or property being purchased.
☐ (brief description of other property).

Filing fees $ _____ **Non-filing insurance** $ _____

Late Charge: If a payment is late, you will be charged $_____/_____% of the payment.

Prepayment: If you pay off early, you
☐ may ☐ will not have to pay a penalty.
☐ may ☐ will not be entitled to a refund of part of the finance charge.

See your contract documents for any additional information about nonpayment, default, any required repayment in full before the scheduled date, and prepayment refunds and penalties.

_____
e means an estimate

State Laws Applicable to Payment Plans

- State law may restrict or prohibit interest/finance charges or fees that can be charged in connection with payment plans, including late payment fees, returned check fees, attorneys' fees and costs incurred in collection.
- Colorado's Uniform Consumer Credit Code requires the provider to register with the Colorado Attorney General if the provider enters into payment agreements with Colorado residents which charge interest or a finance charge.

Federal Affordable Care Act: Limits on Extraordinary Collection Actions

- The regulations implementing the Affordable Care Act prohibit tax-exempt hospitals from engaging in "extraordinary collection actions" (ECAs) against a patient or guarantor to obtain payment for care before the hospital has made reasonable efforts to determine whether the individual is eligible for assistance under the hospital's financial assistance policy (FAP).
  - Selling the debt to another party (with a limited exception)
  - Reporting adverse information about the person to consumer credit reporting agencies or credit bureaus
  - Deferring or denying, or requiring a payment before providing, medically necessary care because of nonpayment of a bill for previously provided care
  - Bringing a court case to collect the patient debt
  - Garnishing an individual's wages, attaching or seizing a bank account, placing or foreclosing on a lien on a person's property, or causing an individual's arrest

Non-Discrimination/Equal Credit Opportunity

- If a patient or obligor requests a payment plan, a provider must not consider any of the following prohibited factors in determining whether, or under what terms, to offer a payment plan:
  - Race
  - Color
  - Sex
    - The CFPB issued an interpretive rule stating that discrimination on the basis of “sex” includes discrimination or discouragement based on sexual orientation and/or gender identity, including discrimination based on actual or perceived nonconformity with sex-based or gender-based stereotypes and discrimination based on an applicant’s associations
  - Religion
  - Marital status
  - National origin
  - Age (if 18 or older)
  - Receipt of public assistance
  - Sexual orientation or gender identity
  - Good faith exercise of rights under Consumer Protection laws
  - Colorado state law expressly prohibits discrimination based upon sexual orientation or gender identity

Adverse Action

- “Adverse action” means the refusal to grant a payment plan requested by an obligor in substantially the amount, or on substantially the terms, applied for by the obligor, unless the provider makes a counteroffer to enter into a payment plan in a different amount or on other terms and the applicant uses or expressly accepts the terms offered.

Adverse Action

- Within 30 days after receiving a completed application for a payment plan, a provider must notify the applicant in writing whether the provider approves the application, makes a counteroffer, or takes adverse action on the application.
- Within 30 days after taking adverse action on an incomplete application for a payment plan, the provider must notify the applicant in writing of the adverse action.

Written Notification of Adverse Action

- Must state:
  - The action taken by the provider
  - A statement of specific reasons for the action taken, or a disclosure of the applicant's right to a statement of specific reasons within 30 days, if the applicant requests it within 60 days of the provider's notification
  - The name and address of the provider
  - "Notice: The Federal Equal Credit Opportunity Act prohibits creditors from discriminating against credit applicants on the basis of race, color, religion, national origin, sex, marital status, age (with certain limited exceptions); because all or part of the applicant's income derives from any public assistance program; or because the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The Federal agency that administers compliance with this law concerning this creditor is the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580."

Cash Payments Over $10,000

- “Cash payments” over $10,000, whether in one or a series of related transactions, must be reported electronically to the federal Financial Crimes Enforcement Network (FinCEN) or on a paper form 8300 to the IRS
- This includes payments in coins, US or foreign currency, cashier’s checks, traveler’s checks and/or money orders

Regulation E

The Electronic Funds Transfers Act (EFTA)

THE ACT:
In 1979, The Electronic Funds Transfer ACT (EFTA), also known as Regulation E, was implemented to protect consumers when they use electronic means to manage their finances.

COVERED TRANSACTIONS:
Payments made by debit card, ACH or electronic check;
Recurring payment withdrawals from a consumer's account

TO STAY COMPLIANT:
Provide specific disclosures before and after taking a payment on-line or over the phone.
Send periodic statements reflecting the covered transaction.

26

NACHA - National Automated Clearinghouse Association

More rules on accepting telephone and on-line payments!

NACHA governs the ACH and its Operating Rules are closely in-line with EFTA. NACHA has provided very clear rules for taking ACH payments, which will ensure compliance with the EFTA.

- The date on or after which the consumer's account will be debited;
- The amount of the debit entry to the consumer's account;
- The consumer's name;
- A telephone number that is available to the consumer and answered during normal business hours for customer inquiries;
- The date of the consumer's oral authorization; and
- A statement by the Originator that the consumer's authorization will be used to originate an ACH debit to the consumer's account.
- All payment call recordings must be retained for a minimum of 2 years under the rule.

Compliance with FDCPA/Regulation F: UDA(A)P Risk

- Make sure your personnel follow the rules of the Fair Debt Collection Practices Act (FDCPA) and CFPB Regulation F, even in attempting to collect the provider's own debt, to avoid risk of unfair, deceptive or abusive act or practice.

Questions?