RURAL HEALTHCARE INITIATIVE

Navigating HIPAA, Breaches of Protected Health Information, and Privacy Laws in Louisiana

Louisiana Rural Health Association

May 31, 2023

Table of Contents

RURAL HEALTHCARE INITIATIVE

RURAL HEALTHCARE INITIATIVE

HIPAA Basics and Louisiana Law

What is “HIPAA”?

- **H**ealth **I**nsurance **P**ortability & **A**ccountability **A**ct of 1996
  - Governs access, use, and disclosure of ***protected health information*** by ***covered entities*** (CE) and ***business associates*** (BA)
  - Intent of HIPAA: protect confidential information in patients’ health records against unauthorized or inappropriate access, use, or disclosure in any form (written, oral, electronic)
- HIPAA Regulations: 45 CFR Parts 160 & 164

What is “Protected Health Information” (PHI)?

- PHI: Individually identifiable health information that is transmitted or maintained in **any** form or medium
  - Individually Identifiable Health Information (IIHI): Information, including demographic information, created or received by a health care provider, health plan, employer, or health care clearinghouse that can be used to identify an individual and that relates to the person’s health care
- **Note: The fact that a person is a patient of a health care provider is itself PHI**

Certain Records Containing IIHI Not Covered by HIPAA

- Records produced by other parties in discovery
- Records obtained from public sources
- Employment records
- Workers' compensation records
- Education records

What is a “Business Associate” (BA)?

- Business Associate: Third party (not an employee of the CE) that creates, receives, maintains, or transmits PHI for/on behalf of CE in the course of providing administrative (not health care) services
- BAs generally must comply with HIPAA Security Rule and most HIPAA Privacy Rule provisions
- CE must enter into a Business Associate Agreement (BAA) with the BA, requiring the BA to follow HIPAA standards and report breaches

What is a “Business Associate” (BA)? (cont’d)

- BAs include the following types of vendors:
  - Health information exchange organizations
  - Other entities that facilitate data transmission services to a CE and require access to PHI on a routine basis
  - Subcontractors that create, receive, maintain, or transmit PHI for/on behalf of the BA
- Record storage companies (paper and cloud) are BAs if they store PHI, whether or not they access the PHI
- Attorneys who receive PHI to provide legal services are BAs

What is a "Business Associate Agreement" (BAA)?

- BAA: A written agreement between the CE and the BA that requires the BA to:
  - Agree to comply with Security Rule
  - Report breaches of unsecured PHI to CEs
  - ***Impose the same restrictions / requirements on subcontractors in writing***
  - If BA carries out CE's obligation under Privacy Rule, BA must comply with applicable Privacy Rule requirements
- **Any time BA will create, receive, maintain, or transmit PHI for/on behalf of CE, you must have a BAA**
- Even if there isn't a BAA in place, BA status—and liability exposure—arises if entity/services provided meet the definition

Key BAA Issues

- BAA must establish how BA is permitted to use and disclose PHI
  - Data aggregation/de-identification/creation of limited data set
  - Management and administration of BA's operations
- BA may not use or disclose PHI other than as permitted or required by BAA or as required by law

Key BAA Issues (cont'd)

- BA must have BAA with its subcontractors who perform a service using PHI:
  - Outside copy services
  - Experts/consultants
  - Technology providers who handle/access data containing PHI
- Reminder: "[E]ach agreement in the business associate chain must be as stringent or more stringent as the agreement above with respect to permissible uses and disclosures"

Key BAA Issues (cont'd)

- Areas to focus on:
  - Specific privacy and security requirements
  - Is data aggregation or de-identification allowed?
  - Are subcontractors permitted? Specific criteria?
  - Indemnification/payment for breach costs/insurance
  - Limitation of liability – if any
  - Timing of breach notification
  - Require encryption of PHI on mobile devices
  - Is offshoring PHI permitted?
  - How much control to exert over BA or subcontractor?

BA Liability

- BAs directly liable for violations of Security Rule
- Security believed to be a major area of non-compliance for many BAs
- Among other things, BAs must:
  - Conduct a Security Rule risk analysis
  - Establish a risk management program
  - Establish written policies and procedures
  - Train employees and workforce
  - Designate a Security Official
  - No obligation to designate a Privacy Official, but some do

What is “De-Identified Information”?

- A data set or record that neither identifies nor can be used to identify an individual
  - De-identified information is not PHI and thus not subject to HIPAA
- Two methods of de-identification:
  - Expert (statistical) determination that risk is small that information could be used to identify the individual
  - Safe Harbor: Removal of 18 identifiers from the record (name, dates, addresses, biometric identifiers, SSNs and MRNs, etc.)

What is a “Limited Data Set”?

- Limited Data Set (LDS): De-identification “lite”; can use LDS for research, public health, and health care operations
  - Dates, certain geographic information (city/state/zip) can remain
  - Limited data sets are considered PHI if DOB and zip code are not removed
- **Note: A BA that prepares an LDS for or receives an LDS from a CE must enter into a Data Use Agreement with CE**
  - Data Use Agreement is like a BAA “lite”

Uses and Disclosures of PHI

- CEs and BAs may only use or disclose PHI as permitted or required by law
- In general, CE or BA can disclose PHI:
  - To the patient
  - For treatment, payment, and health care operations
  - Pursuant to written authorization of patient
  - To law enforcement in certain circumstances
  - As required by law (e.g., public health, health care oversight, legal process (search warrant))
- **A BA may use and disclose PHI only as permitted by its BAA or as required by law**

Minimum Necessary Standard

- Minimum Necessary: Except where PHI is used/disclosed for treatment, CE or BA may use or disclose only the minimum PHI necessary to accomplish the purpose of the use or disclosure
  - Example: State law requires reporting of gunshot wounds to law enforcement. Report must include patient's name, age, sex, race, residence or present location, and character/extent of injury. (La. Rev. Stat. § 14:403.5)
  - Disclosure of any additional information is a violation of minimum necessary

HIPAA Preemption Rules

- HIPAA Preemption: If HIPAA and State law are inconsistent, follow law that is **more stringent** (provides most protection for privacy of patient's PHI **or** permits greater rights of access to/amendment of PHI by subject of PHI)
  - Some state laws are much more protective of patient privacy in almost all situations (i.e., limited disclosure to patient consent/court order situations only)
  - Certain types of information (behavioral health, AIDS/HIV) are subject to higher levels of confidentiality

Louisiana Law Requirements

- The Louisiana Consumer Privacy Act (SB 199) was introduced and is in committee review – it has not yet been passed
- A patient's health data (diagnosis, treatment, or health) held by a health maintenance organization generally must be kept confidential (La. Rev. Stat. § 22:265 of Title 22)
- In addition:
  - La. Rev. Stat. § 40:1171.4 of Title 40 provides for the confidentiality of HIV test results;
  - La. Rev. Stat. § 40:2144 of Title 40 ('Hospital Records and Retention Act') provides patients with statutory rights of access to medical records; and
  - Article 510 of the Code of Evidence provides for a healthcare provider-patient privilege, which may be waived in cases involving child abuse or molestation

HIPAA Waivers – Telehealth

- With the end of the COVID-19 PHE on May 11, 2023 the U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced that its enforcement discretion regarding violations of HIPAA, applicable during the PHE, also would be coming to an end.
- Covered entities and business associates now have a 90-day transition period, ending on August 9, 2023, in which to bring their telehealth practices into compliance with the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (HIPAA Rules). Among other things, this will require entities that may be using telehealth technologies provided by companies that will not agree to sign BAAs or switch to platforms offered by companies that do.
- Providers using telehealth should take advantage of the transition period to:
  - Review their telehealth operations—including their arrangements with their telehealth technology vendors
  - Identify HIPAA-compliant telehealth vendors and enter into BAAs with such vendors
  - Take steps to ensure that their provision of telehealth services complies in all respects with the HIPAA Rules

RURAL HEALTHCARE INITIATIVE

Breach Notification: Federal and State

What is a “Breach”?

- “Breach”
  - acquisition, access, use, or disclosure
  - of unsecured PHI
  - not permitted by Privacy Rule
  - that compromises security or privacy of PHI
- “Unsecured PHI”: PHI that has not been encrypted or destroyed in compliance with HHS guidance

Breach Examples

- Looking up and sharing an individual's health record outside of the normal course of treatment (e.g., snooping in the medical records of celebrity patients)
- "Hacking" incidents (phishing, spoofing, baiting, etc.)
- Misdirected information due to human error (typing in the wrong fax number, printing out Patient A's discharge summary and handing to Patient B)
- Lost/misplaced **unencrypted** laptops and USBs

Breach Notification: Federal

- HITECH requirements must be compared to existing state breach notification requirements and, if they don't conflict, both rules must be followed
  - HITECH applies to breaches of certain clinical and financial information

Breach Notification: Louisiana

- The Database Security Breach Notification Law, under §§ 51:3071 to 51:3077 of Title 51 of the Louisiana Revised Statutes (La. Rev. Stat.) was enacted in 2005, became effective on 1 January 2006, and was amended effective 1 August 2018.
- Pursuant to La. Rev. Stat. § 51:3074, the notification obligations under the Database Security Breach Notification Law apply to all persons and legal entities that own or license computerized data that includes Louisiana residents' personal information (La. Rev. Stat. § 51:3074(C)). In cases where the breach involves computerized data that the person or agency does not own, then the person or agency must notify the owner (La. Rev. Stat. § 51:3074(D)).
- When a data breach results in 'personal information' being acquired and accessed by a third party without authorization, the Database Security Breach Notification Law generally requires notice to affected individuals and the Louisiana Attorney General ('AG'). 'Personal information' includes the resident's last name and first name or first initial, in combination with one or more of the following data elements:
  - social security number;
  - driver's license number or state identification card number;
  - account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
  - passport number; and
  - biometric data, including fingerprints and other unique biological characteristics used to authenticate an individual's identity to access a system or account

Breach Notification: Louisiana (cont'd)

- The definition of PHI excludes 'publicly available information that is lawfully made available to the general public from federal, state, or local government records' (La. Rev. Stat. § 51:3073(4)(b)).
- The protection for loss of 'personal information' under La. Rev. Stat. § 51:3073(4)(a) extends only to Louisiana residents. However, **no notification is required if the information was encrypted or redacted, or if there is no reasonable likelihood of harm to the affected individuals**.
- According to regulations promulgated by the Louisiana AG, failure to give timely notice to the Louisiana AG may result in fines of up to $5,000 per day, pursuant to § 701 of Title 16 of the Louisiana Administrative Code (La. Admin. Code).
- Unlike many other breach notification laws, Louisiana's law creates a **private right of action** for persons harmed by violations of the Database Security Breach Notification Law, including the right to recover actual damages for failure to give timely notice under the Database Security Breach Notification Law (La. Rev. Stat. §§ 51:3074(J) and 51:3075).

Consequences of Breach of Unsecured PHI

- "Without unreasonable delay," but no more than 60 days after a CE or BA discovers a breach, CE or BA must:
  - Notify each person whose unsecured PHI has been improperly accessed, acquired, used, or disclosed as a result
  - Notify the Secretary of HHS
    - Within 60 days of discovery, if the breach affected more than 500 individuals
    - Within 60 days of the end of the calendar year, for each breach affecting fewer than 500 individuals
  - For breaches affecting more than 500 individuals:
    - Notify prominent media outlets serving the area

Is it a Breach?

- Should not assume every impermissible use/disclosure of PHI is a "breach"
- An impermissible use/disclosure is not a breach:
  - When the PHI is properly encrypted/destroyed
  - When the use/disclosure is permitted under HIPAA
  - When a breach exception applies
  - When a low probability exists that privacy or security of data is compromised

Exceptions to Breach

- HITECH contains three narrowly-construed exceptions:
  - Unintentional acquisition/access/use of PHI at CE/BA
  - Inadvertent disclosure of PHI within CE/BA
  - Recipient would not reasonably be able to retain PHI
- If an acquisition, access, use, or disclosure fits within an exception, it is not a breach, ***even if*** information was unsecured PHI and ***even if*** the disclosure is not permitted under HIPAA
- If potential breach fits within an exception, ***no notice is required*** to the government, the patient, or the media

Risk Assessment

- Impermissible access, use, or disclosure of PHI is ***presumed*** a breach ***unless*** CE or BA shows a "low probability" that PHI has been "compromised"
  - No definition of "compromised" (OIG promised but has not provided guidance)
- Determine probability of compromise by performing a Risk Assessment
  - Good faith, thorough assessment of overall probability required
  - Conclusions drawn must be reasonable
- NOTE: may notify without performing Risk Assessment

Risk Assessment

- Risk Assessment requires consideration of at least:
  - Nature and extent of PHI involved
  - Unauthorized user or recipient of PHI
  - Whether PHI was actually acquired or viewed
  - Extent to which risk to PHI was mitigated
- Risk Assessment may consider other factors

Risk Assessment

- Minimum necessary violations and improper uses/disclosures within CE/BA require risk assessments
- However, due to presumption of breach, risk assessments are now "voluntary"
  - CEs and BAs may skip risk assessment and proceed directly to make breach notifications
- If decide to perform risk assessment, "show your math"
- Following potential breach, always take and document corrective action—HHS more likely to refrain from formal enforcement

RURAL HEALTHCARE INITIATIVE

Compliance with Limited Resources

Key Strategies for Compliance

- HIPAA compliance is essential for healthcare providers to protect patient privacy and avoid potential legal and financial consequences. While limited resources can present challenges, there are several steps healthcare providers can take to comply with HIPAA effectively:

1. **Educate Staff**: Ensure that all staff members receive training on HIPAA requirements, including the Privacy Rule, Security Rule, and Breach Notification Rule.
   - Free HIPAA training and resource materials are available online, such as the OCR's Summary of HIPAA Privacy Rule and the HHS's HIPAA Guidance Materials.
2. **Conduct Risk Assessments**: Perform regular risk assessments to identify vulnerabilities and potential risks to the security of PHI. Prioritize risks based on severity and address them accordingly, even with limited resources.
   - Recommend performing assessments at least annually.
3. **Develop Policies and Procedures**: Create comprehensive policies and procedures that outline how PHI should be handled, stored, and transmitted securely (access controls, data encryption, password policies, proper disposal methods).

Key Strategies for Compliance (cont'd)

1. **Implement Physical Safeguards**: Implement physical safeguards to secure areas where PHI is stored or accessed (locked storage areas, restricted access to PHI, surveillance systems, proper disposal of physical documents).
2. **Implement Technical Safeguards**: Utilize technical measures to protect PHI in electronic form (secure networks, firewalls, encryption, strong authentication methods, regularly updating software and systems to address vulnerabilities).
3. **Limit PHI Access**: Implement appropriate access controls and user authentication mechanisms to ensure that only authorized individuals have access to PHI.
   - Restrict access based on the principle of "least privilege" - only the minimum necessary information for staff members to perform their job responsibilities.
4. **Train Employees on Security**: Provide ongoing training to staff regarding security best practices (avoiding phishing e-mails, recognizing potential security threats, reporting any suspicious activity promptly).

Key Strategies for Compliance (cont'd)

1. **Monitor and Audit**: Regularly monitor and audit systems, networks, and access logs to detect any unauthorized access or breaches promptly. This helps in identifying and addressing security incidents promptly, reducing the impact on patient privacy.
   - Recommended to perform audits at least annually.
2. **Establish Business Associate Agreements**: Ensure that any external entities or vendors that handle PHI on behalf of the healthcare provider sign appropriate BAAs.
   - The U.S. Department of Health and Human Services (HHS) offers free template BAAs, found here.
3. **Document Policies and Procedures**: Maintain detailed documentation of all policies, procedures, risk assessments, and training sessions conducted.
   - Demonstrates the organization's commitment to compliance and serves as a reference for staff and auditors.

- HIPAA compliance is an **ongoing process** – requires continuous efforts to address evolving security risks.
- Compliance posture can and should be improved over time.

RURAL HEALTHCARE INITIATIVE

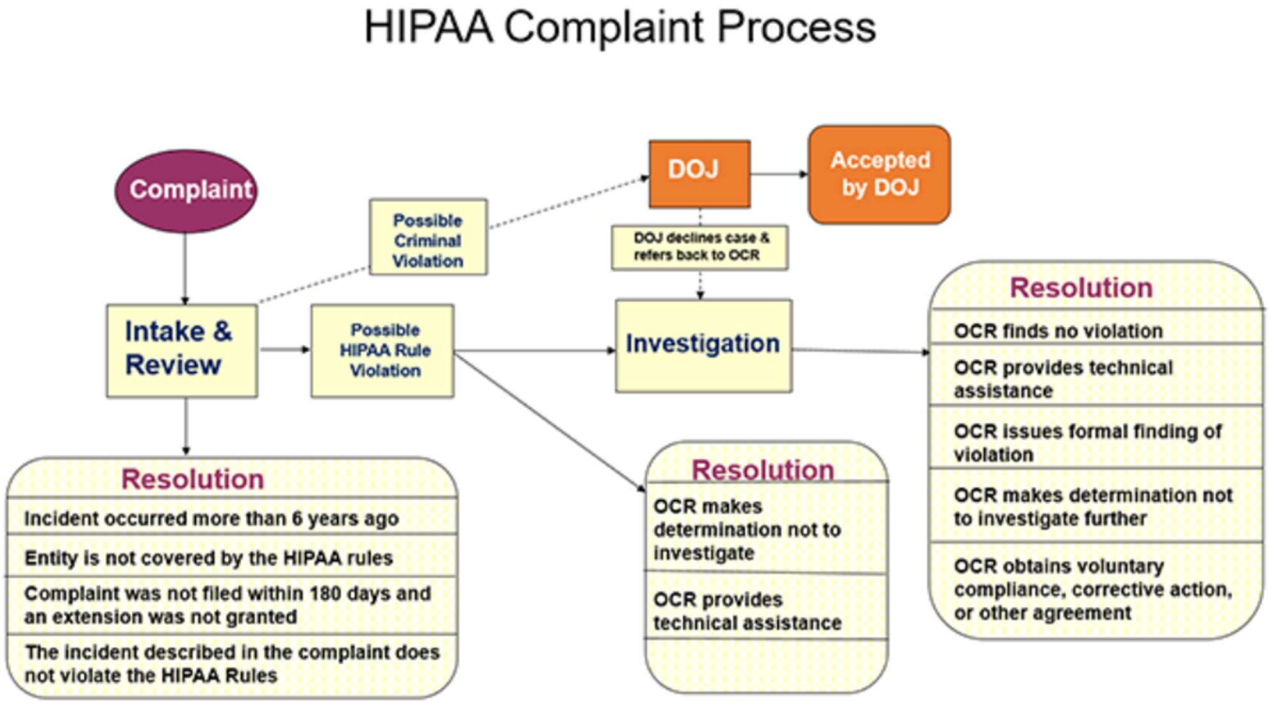
Liability and Enforcement Examples

Lawsuits for HIPAA Violations

- Still no private right of action under HIPAA (i.e., patient cannot sue CE or BA directly for HIPAA violations)
- However, state law claims for negligence, invasion of privacy based on HIPAA violations have been successful
- Class action suits for HIPAA violations typically dismissed if no damages have accrued—but damages are arising
- State Attorneys General can bring action on behalf of patients for HIPAA violations seeking injunctive relief and damages
- CE can sue BA for violation of BAA → follow your BAA!

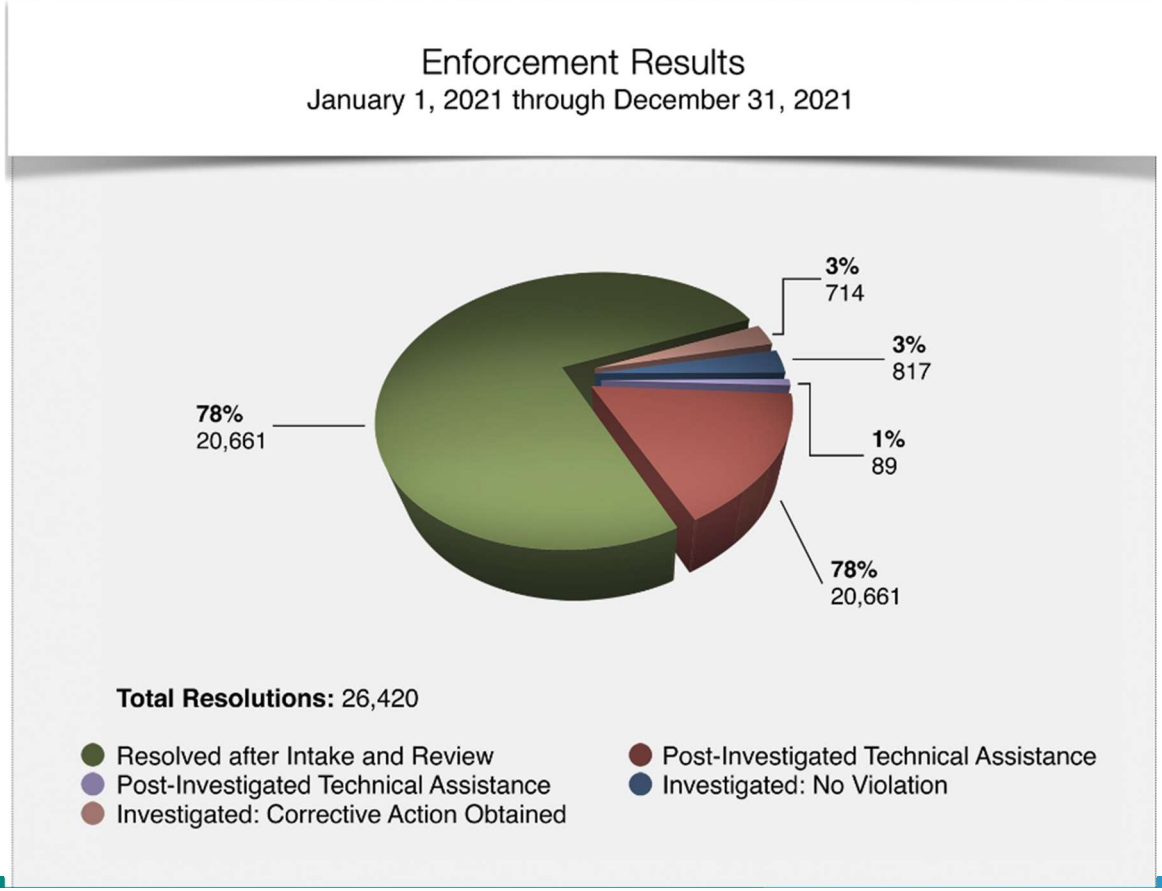
Regulatory Enforcement

- HHS Office for Civil Rights (OCR): Agency responsible for enforcing HIPAA Privacy and Security Rules



RURAL HEALTHCARE INITIATIVE

Regulatory Enforcement



RURAL HEALTHCARE INITIATIVE

Regulatory Enforcement – Case Examples

- Banner Health: Settlement with Arizona hospital system following hacking incident which disclosed PHI of 2.81 million customers; penalties due to lack of risk assessment, insufficient monitoring and security compliance, and lack of encryption during PHI transmission. $1,250,000 penalty and Corrective Action Plan (CAP)
- Life Hope Labs: Settlement with diagnostic laboratory due to failure to provide patient access to records in a timely manner. $16,500 penalty and CAP
- New Vision Dental: Settlement with dental practice due to impermissible disclosure of PHI in response to online reviews. $23,000 penalty and CAP

RURAL HEALTHCARE INITIATIVE

Regulatory Enforcement – Case Examples

- Hospice of North Idaho: Settlement following theft of unencrypted laptop containing ePHI of 441 individuals; penalties due to lack of risk assessment, lack of security rule compliance, no encryption. $50,000 penalty and CAP
- Dental Settlements: Settlements with three dental practices due to failure to provide patient access to records. Penalties ranged from $25,000 to $80,000; CAPs
- NE Dermatology: Settlement due to disposal of empty specimen containers labeled with patients' information in unsecured dumpster. $300,640 penalty and CAP

Regulatory Enforcement – Case Examples

- OSU: Settlement with OSU's Center for Health Sciences, which experienced a breach affecting 279,865 individuals after malware was uploaded to a web server where staff had improperly stored folders containing PHI. OSU failed to have appropriate risk assessment and security rule compliance, failed to provide appropriate breach notification. $875,000 penalty and CAP
- Premera Blue Cross: Settlement with insurer who reported phishing attack that disclosed ePHI of 10,466,692 individuals; failure to conduct appropriate risk assessment and implement appropriate security measures. $6,850,000 penalty and CAP

Questions?

Robert L. Wilson, Jr.
Nelson Mullins
301 Hillsborough Street
Raleigh, North Carolina 27603
bob.wilson@nelsonmullins.com

RURAL HEALTHCARE INITIATIVE