Based on the **NCSW Circular for Mandatory Data Reporting** and the **NGDRS Architectural Framework**, the system utilizes a **"Unified Intake, Divergent Investigation"** model.
Here is the step-by-step explanation of the generic workflow shared by all cases, followed by the specific workflows for Physical GBV and Digital TFGBV.

Part 1: The Generic Workflow (Shared Pipeline)

This process is mandatory for all reporting entities (Police, Health, Social Welfare) to ensure every survivor is counted, regardless of where they first seek help ("No Wrong Door Policy") 1, 2.

Step 1: Intake & Digital Registration (The Entry)

1. **Department:** District Focal Point (Police Station, Hospital, or Shelter).
2. **Time Limit:** Must be completed within **24 hours** of the survivor's arrival 3.
3. **Actions:**
4. **Generate ID:** The system assigns a unique, anonymized **Case_ID** (e.g., PB-LHR-2025-001) 3.
5. **Tagging:** The officer selects the Crime_Type from a standardized dropdown (GBVIMS standards) to classify it as Physical (e.g., GB-SX) or Digital (e.g., TF-A4) 3, 4.
6. **Safety Check:** If immediate danger is detected (e.g., weapon involved), a "Lethality Assessment" triggers a referral to a Shelter 2.

Step 2: Triangulation & Validation (The Quality Check)

- **Department:** District/Provincial Reviewer (Women Development Department).
- **Time Limit:** Continuous (Corrective actions within **72 hours**) 5.
- **Actions:**
- **Cross-Check:** The system compares data across departments.
- *Example:* If Police report 5 rapes, but Health reports 0 medical exams, the system flags a **"Data Mismatch Alert"** 5.
- **Correction:** The record is locked and sent back to the origin office for rectification 6.

Step 3: Submission & Aggregation

1. **Department:** Provincial Focal Point.
2. **Deadline:** Monthly reports submitted by the **10th**; Quarterly briefs by the **15th** 7, 8.
3. **Actions:**
4. **Certification:** The Provincial Officer digitally signs the master sheet.
5. **Upload:** Data is transmitted to the Central NCSW Database 6.

Step 4: National Analysis & Alerts

1. **Department:** NCSW (National Commission on the Status of Women).
2. **Actions:**
3. **Red Zone Calculation:** If a district shows >50 cases/100,000 people or a >25% spike, the system triggers an **Emergency Alert** to the Chief Secretary 7.

4. **Anonymization:** All names/addresses are stripped before the data hits the National Dashboard to protect survivor privacy 9, 10.

Part 2: Divergent Workflows (Specific to Crime Type)

Once the case is registered, the system uses **"Jurisdictional Routing Logic"** to send the case down different investigation paths 11, 12.

Workflow A: Physical/Medico-Legal (e.g., Rape, Domestic Violence)

Primary Departments: Provincial Police, Health Dept, Prosecution.

- **Step 1: Police Action (FIR Registration)**
- **System Logic:** If the crime is **Rape (Section 375/376)**, the system **blocks** the "Mediation/Compromise" button because the crime is Non-Compoundable 12.
- **Action:** Police must register the FIR immediately.
- **Step 2: Health Department Action (Medical Exam)**
- **System Logic:** The system triggers a **72-Hour Countdown Timer** for DNA collection 2.
- **Action:** Medico-Legal Officers (MLOs) conduct the exam.
- **Constraint:** The system blocks entry of the illegal "Two-Finger Test" results, enforcing modern protocols 2.
- **Step 3: Social Welfare Action (Shelter)**
- **System Logic:** Based on the survivor's location, the system auto-populates the nearest **Dar-ul-Aman** (Shelter) 2.
- **Action:** Shelter staff record services provided (Psychosocial support, Legal Aid) in the *Service_Provision* module 13.
- **Step 4: Prosecution Action (Trial)**
- **Action:** Prosecutors update the *Justice_Funnel* module (Challan Submitted $\rightarrow$ Trial $\rightarrow$ Conviction) 13.

Workflow B: Digital/TFGBV (e.g., Deepfakes, Cyberstalking)

Primary Departments: NCCIA, SMRA, Federal Courts.

- **Step 1: NCCIA Action (Investigation)**
- **System Logic:** The system detects a Digital Code (e.g., **TF-A4 Deepfake**) and routes the ticket *away* from local police directly to the **National Cyber Crime Investigation Agency (NCCIA)** 11, 12.
- **Action:** NCCIA agents receive the file and begin tracing IP addresses.
- **Step 2: Evidence Preservation (Hashing)**
- **Action:** The Intake Officer uploads screenshots/URLs.
- **System Logic:** The system generates a **Cryptographic Hash** of the evidence to create a tamper-proof "Chain of Custody" for the courts 4, 14.
- **Step 3: SMRA Action (Platform Takedown)**
- **Department:** Social Media Protection & Regulatory Authority (SMRA).
- **Action:** A sub-ticket is sent to the social media platform (e.g., TikTok, Meta).
- **Metric:** The system tracks Takedown_Time_Hours to measure if the platform complied within 24 hours 11, 13.

- **Step 4: Court Action (Adjudication)**
- **Action:** The judge records if the digital evidence was **Accepted** or **Rejected**, helping identify gaps in forensic training 15.

Workflow C: Hybrid/Cross-Jurisdictional (e.g., Sextortion)

Primary Departments: Joint Task Force (Police + NCCIA).

- **Step 1: Dual Routing**
- **System Logic:** If the crime involves *physical* threats facilitated by *tech* (e.g., "Sextortion" TF-A8), the system triggers a **Joint Alert** 12.
- **Step 2: Parallel Action**
- **NCCIA:** Works to remove the content online.
- **Provincial Police:** Works to arrest the extortionist on the ground.
- **Step 3: Consolidated Reporting**
- Both departments update the same Case_ID so the Prosecutor receives a single, unified file containing both the digital forensics and the arrest report 12.